UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

OSR ENTERPRISES AG and OSR R&D ISRAEL LTD.,

Plaintiffs,

-against-

REE AUTOMOTIVE LTD., REE AUTOMOTIVE HOLDING, INC. and REE AUTOMOTIVE USA INC.,

Defendants.

Case No.:

COMPLAINT FOR PERMANENT INJUNCTIVE AND OTHER RELIEF

JURY TRIAL DEMANDED

Plaintiffs OSR Enterprises AG ("OSR Enterprises") and OSR R&D Israel Ltd. ("OSR R&D" and, together with OSR Enterprises, "OSR"), as and for their complaint against REE Automotive Ltd. ("REE Automotive"), REE Automotive Holding, Inc. ("REE Holding") f/k/a 10X Capital Venture Acquisition Corp. ("10X"), and REE Automotive USA Inc. (together "Defendants" or "REE"), allege as follows:

NATURE OF THE ACTION

1. This is a trade secret misappropriation action against REE, a former wheelchair maker that stole technology—including source code and other proprietary files—worth billions of dollars from OSR to transform itself into a developer of a platform for electric vehicles ("EV"). REE sought to enter the EV sector so that it could take advantage of the strong interest in EV technology from publicly-traded Special Purpose Acquisition Companies or "SPACs." Merging with a SPAC would allow REE to raise hundreds of millions of dollars and go public quickly and with little oversight. With this goal, REE had struggled for years to repurpose its concept for in-wheel wheelchair suspension into a rudimentary and largely mechanical decentralized system to house EV components in the wheel ("REE Platform"), before watching its aspirations disintegrate as competitors beat it to market.

2. Unfortunately for REE, SPACs—including 10X, the SPAC with which REE ultimately merged—were not interested in a company with a low-tech EV platform, much less one that was undifferentiated from competitors' offerings. So REE hatched a plan to steal from the sort of cutting-edge automotive technology company that it had dreamed of becoming—in this case, OSR, which had created, among other things, a revolutionary way to control autonomous vehicles through a centralized processing unit with advanced artificial intelligence, data science, and processing capabilities.

3. REE induced at least nine former OSR employees to join REE in breach of their contractual agreements with, and fiduciary duties to, OSR. The first employee was OSR R&D's head of research and development, Ohad Stauber, who became REE's own head of research and development.

4. Just prior to leaving, Stauber copied from OSR's systems to his OSR laptop and external drives on several occasions, over 100,000 files, including, among other things, source code, AI algorithms, design schematics**,** data sheets, customer information, and market and technical research. Stauber also had used a personal phone to take pictures of OSR's secret technology and circuit boards.

5. REE used that stolen data in its products and marketing literature. Just one year after REE recruited OSR's employees, REE dramatically changed the descriptions of its prototype REE Platform, representing a stunning, and implausibly rapid, reversal of its core business model. Rather than marketing a mechanical, decentralized in-wheel system for EVs, REE pivoted its business model to a centralized AI computer platform with the advanced capabilities stolen from, and precisely mirroring, OSR's technology embodied in the stolen files.

6. Despite OSR's repeated written warnings to cease and desist such theft, REE passed off to investors OSR's technology as REE's own to differentiate itself in a race to go public and use the proceeds to reach the critical U.S. market with technology built from OSR's trade secrets.

7. On December 14, 2022, an Israeli police officer confirmed to OSR that there is an investigation "currently being conducted" by a special team of the Israeli police's cybercrime division "against Ohad Stauber and REE corporation, inter alia, under suspicion of theft and computer crimes."[1]

[1] Translated from Hebrew.

8. In light of REE's unlawful actions, OSR has been left with no choice but to bring this action to seek monetary damages and injunctive relief to prevent REE from further unfairly benefitting from OSR's investment of more than a decade in developing and producing its proprietary and highly regarded EVOLVER platform.

* * *

OSR's EVOLVER—the "Central Brain" for Vehicles

9. Beginning in 2011, Orit Shifman—the founder, Chairman and CEO of OSR Enterprises AG—anticipated the automotive market's need for a single, unified computer system with robust data collection and processing and advanced AI technology to control all of the many complex processes involved in driving the next generation autonomous car. OSR's vision was revolutionary. Before OSR, no one in the market had pursued a centralized control system capable of harmonizing the vast amount of data from all of the many different driving processes. OSR spent nearly a decade, employing more than 150 employees, working millions of hours and spending well over $100 million on building its hardware and software product, the "EVOLVER."

10. Among other technologies, OSR built from scratch a proprietary AI "neural network"—a complex amalgamation of algorithms that OSR programmed and trained to interact with one another, not only to make complex decisions independently, but to continuously learn how to make those decisions better. To feed that neural network, the EVOLVER is also capable of collecting, storing, and processing tens of thousands of data points in real time.

11. With its capabilities in data storage and processing and advanced AI, the EVOLVER has made quantum leaps in a variety of technological applications, including in independently making—and rapidly executing—the incredibly complex decisions necessary to drive a car autonomously. The EVOLVER also contains groundbreaking developments in automotive safety. For example, the EVOLVER can alert the driver of pedestrians in a blind spot

and calculate their velocity and vector, and even whether they are distracted by a smartphone, to determine whether there is a collision risk. The EVOLVER can switch from manual to autonomous driving to avoid hazards by analyzing data from camera feeds, as well as countless other sources, to detect the driver's emotions and attention or even medical emergencies—including based on the driver's facial expressions, her braking and acceleration pressure and patterns, whether her calendar indicates that she is late for a meeting, and whether there are upset children in the car. And the EVOLVER can draw distinctions and reach conclusions from data that allows it to adapt either universally to all drivers using OSR's connected system or be tailored to the individual driver, in order to evolve.

12. The EVOLVER is also capable of rapidly gathering, processing, and analyzing enormous amounts of data to perform what OSR calls "multi-domain" and "data-as-a-service" functions. The EVOLVER can optimize driving routes depending on, for example, predictions it makes based on current and historical traffic patterns, time of day, and weather. And it can monetize driving data by, for example, providing insurers with information, managing commercial fleets of vehicles, and recommending preventative maintenance by analyzing driving conditions and mechanical data.

13. OSR's vision and investment has paid off. Since 2016, OSR has supplied its technology to some of the world's largest automakers, in order to integrate it into future vehicles. For example, OSR entered into a collaboration with Jaguar-Land Rover ("Jaguar") to enhance automated drive and secure connected technologies through integrating the EVOLVER with Jaguar's EV, the I-PACE, which was made public in 2019 at the International Automobil-Ausstellung ("IAA") show in Germany. And in around two years, OSR plans to have its own cutting-edge fully electric vehicle in production based on the latest version of the EVOLVER.

14. OSR's technology necessarily derives its immense value from being kept secret given the highly competitive and rapidly developing electric vehicle and autonomous driving space. To that end, OSR implements stringent, best-in-class security policies.

REE's Decentralized In-Wheel Platform

15. Unlike OSR, REE was all about mechanics, with no experience in the type of advanced computing that is at the heart of EVOLVER. REE was founded in 2011 as "SoftWheel" to sell a mechanical suspension system for wheelchairs. SoftWheel changed its name to "REE" when it publicly entered the automotive space for the first time in June 2019, after seeing an opportunity in the recent flood of investment money in the United States flowing to the EV sector.

16. REE announced then that it was developing a "REE Platform," which at the time consisted of the REEboard—a flat metal chassis known in the industry as a "skateboard" that is ubiquitous in the EV industry—and the REEcorners—a system that houses the car's motors and other major components in the wheel hubs. Not only did the REE Platform lack a central processing system capable of controlling the many aspects of a vehicle—a core achievement represented in the EVOLVER—but REE touted the REEcorners' modular, *decentralized* nature as the core tenet of its business model. REE's motto was "put it all in the wheel[s]."

17. Despite all of REE's promises to investors of cutting-edge developments, REE was struggling for relevance as competitors were beating it to market with functionally identical but technologically superior concepts. Investors noticed. For example, REE struggled to respond when one analyst pointed out that "there's a lot of other skateboards out there."

REE Steals OSR's Proprietary Technology

18. In its desperation to differentiate itself and live up to its promises to investors, employees, and the public of delivering a revolutionary system, REE hatched a plan to

systematically steal its way to the type of cutting-edge technology company it had aspired to be: OSR.

19. REE first set out to aggressively recruit as many of OSR's R&D employees as possible. REE did this knowing that those employees were contractually restricted from working at REE and bound by their duties of confidentiality, because, after OSR became aware of REE's efforts, it told REE as much.

20. REE had its first success in or around the Fall of 2019, when REE recruited the head of OSR R&D's research and development team, Ohad Stauber, to head its own research and development efforts. REE was not attracted to Stauber himself. Stauber had only two years of automotive experience working for OSR; his prior background was in three-dimensional mapping. This experience has little relevance to REE's modular, "dumb" EV platform. Rather, REE wanted Stauber because of his knowledge of, and access to, OSR's technology.

21. In September 2019, several days after researching REE on his OSR laptop, and almost certainly talking to REE (OSR later learned that REE had been actively seeking to recruit OSR employees since at least as early as July 2019), Stauber went to a tradeshow where certain of OSR's data would, for a short time, be outside of OSR's closed system and more vulnerable to copying. Stauber copied to a high-capacity external drive that he had brought for the purpose a folder containing OSR's proprietary source code for the EVOLVER, configurations OSR had created for customers, and other proprietary data.

22. All in all, a forensic analysis OSR conducted revealed that, over several occasions, Stauber had copied from OSR's systems to his OSR laptop and external drives over 100,000 files, consisting of over 20 gigabytes of OSR's proprietary data, including, among other things, source code, AI algorithms, design schematics**,** data sheets, customer information, lists of components

and schematics, and market and technical research. OSR also learned that Stauber had used a personal phone to take pictures of the inside of OSR's secret technology and circuit boards—which also violated OSR's security policies.

23. In early November 2019, only several weeks after returning from the tradeshow, Stauber drove to REE's offices and days later, announced his resignation. Two days after that, in a failed attempt to cover his tracks, Stauber deleted the files from his OSR laptop.

24. OSR, through counsel, notified REE that Stauber had stolen its trade secrets and was violating the terms of his employment agreement. Rather than take corrective action, however, REE and Stauber conspired to recruit as many of OSR's research and development employees as possible. They ultimately persuaded at least eight additional high-ranking employees to resign and collaborate with REE, in breach of their fiduciary obligations to and agreements with OSR, to make use of their knowledge of OSR's trade secrets.

REE Changes its Business Model

25. With this treasure trove of OSR's secret technology, only a year after Stauber joined REE, REE was able to announce an impossibly rapid transformation of, and 180-degree pivot from, its core business model. REE's rudimentary mechanical system, the main purported advantage of which had been decentralization, would now suddenly include an advanced, central AI computer processor with a suite of capabilities all directly mirroring OSR's EVOLVER.

26. Specifically, in early 2021, REE announced that the REE Platform would now contain the "REEcenter." Like the EVOLVER, the REEcenter acts to centrally control the other main components of the REE Platform using AI. And, just like the EVOLVER, the REEcenter purportedly provides for autonomous driving and AI-driven computerized decision-making, and collects and processes driver data to monetize it for the purposes of insurance, preventative

maintenance, and vehicular fleet management—the precise "multi-domain," data-as-a-service capabilities of the EVOLVER.

27. Reflecting the brazenness of its theft, REE even adopted OSR's precise marketing terminology, referring to the REEcenter as the "central brain" for cars—how OSR refers to the EVOLVER—and stating that it offers customers the "Freedom to Create"—OSR's own tagline.

28. That REE could develop the REEcenter in a year without the benefit of OSR's trade secrets is inconceivable. Creating a central computer for a car with these advanced vehicular control capabilities is extremely difficult, time-intensive, and expensive, necessarily requiring massive data collection and iterative development that must span years. REE had no prior experience in these fields. And when REE hired Stauber, REE only had about 35 employees across all disciplines—in contrast to OSR's approximately 150 employees and decade of development—who would be entirely incapable of such technological leaps in such a short time.

REE Leverages OSR's Technology To Go Public

29. With the benefit of OSR's technology, REE was finally able to obtain the SPAC financing it coveted. In December 2020, only weeks before REE publicly announced the REEcenter, REE formally entered into discussions with 10X—the predecessor to defendant REE Holding—for a merger that would make REE publicly traded on the NASDAQ and yield it $500 million in cash to enable it to produce the REE Platform (the "Merger").

30. REE used OSR's trade secrets to market itself to 10X. In seeking a company to merger with, 10X had "focus[ed] [its] efforts . . . on technology paradigms including artificial intelligence ('AI'), automation, data science, ecommerce and Software-as-a-Service ('SaaS')." This vision, while bearing little resemblance to REE's original platform, described precisely OSR's AI platform with its strong data science and data-as-a-service offerings.

31. In February 2021, REE and 10X jointly announced that they had agreed to enter into the Merger. 10X and REE's public disclosures to investors emphasized the value of OSR's technology as a "critical part of the REEplatform design [that] will offer a number of significant advantages," including "paving the way for advanced autonomous driving strategy." Among REE's "competitive strengths" were the REE Platform's "predictive maintenance . . . through . . . AI" and "data harvesting capabilities"—all developed by misappropriating OSR's trade secrets.

32. When OSR again sent demand letters to REE and 10X warning that their technology was stolen from OSR, REE did not (and could not) attempt to rebut OSR's allegations that Stauber had stolen data or deny that they had systematically targeted OSR's employees. REE could only point to evidence that, prior to Stauber joining the company, it had been working on putting car components in the wheel. But REE did not contest that the major technological leaps in centralized computing, data processing and collection, AI, and "multi-dimensional" services—identical to OSR's capabilities—only began *after* Stauber came to REE with the stolen files.

33. During this time, REE entirely failed to disclose its theft, or even the mere existence of OSR's demand letters, to prospective partners, the public, the SEC, or most investors, passing off the stolen technology as its own. To the contrary, REE's disclosures repeatedly referenced its purportedly own "proprietary" technology when the technology it was touting as its competitive advantage was based, in its entirety, on OSR's trade secrets. In fact, REE represented to its investors that all of its intellectual property was its own—when it actually belonged to OSR. REE also represented, in a merger agreement attached to its proxy statement, and in a later registration statement, that there had been no material threatened litigation. Thus, REE's substantial fundraising was based on trade secrets stolen from OSR.

34. Apparently some select investors, however, did receive notice. By the time of the Merger, less than two weeks after OSR sent a letter to 10X, $150 million of the $500 million of initial investments were redeemed. REE and 10X replaced this cash with funds from a few large institutional investors, whom they kept in the dark. These redemptions represent an unusually large percentage of the initial investors, approximately 75%, and were mostly by large institutions and professional investors.

35. Backed with hundreds of millions of dollars in funding, REE continues to threaten further disclosures of OSR's technology, including by entering into partnerships to produce its platform based on OSR's technology. For example, in November 2021, REE announced a new autonomous, delivery fleet vehicle, called the REE Leopard. And in 2022, REE announced that it has partnered with Texas-based EAVX to produce an EV van based on OSR's trade secrets.

36. Accordingly, through this lawsuit, OSR seeks injunctive relief and recovery of damages that it has suffered as a result of REE's misappropriation of OSR's trade secrets, under the Defend Trade Secrets Act of 2016, 18 U.S.C. § 1836(b)(1), the Texas Uniform Trade Secrets Act, and REE's unfair competition. Unless REE's actions are halted, OSR will continue to suffer irreparable damage.

THE PARTIES

37. Plaintiff OSR Enterprises is a corporation organized under the laws of Switzerland, with its principal place of business at Zugerstrasse 6, 6330 Cham, Switzerland. Its corporate headquarters are located at Suurstoffi 41, 6343 Rotkreuz, Switzerland.

38. Plaintiff OSR R&D is a corporation organized under the laws of Israel, with its principal place of business at Ef'al Street 25, Petah Tikva, Israel. OSR R&D is a wholly-owned subsidiary of OSR R&D GmbH, which is a wholly-owned subsidiary of OSR Enterprises. OSR Enterprises engaged OSR R&D to perform research and development services on OSR

Enterprises' behalf, pursuant to confidentiality agreements. Together, OSR Enterprises, OSR R&D, and their subsidiaries research and develop technology for creating the EVOLVER and other technologies for smart, networked autonomous cars.

39. Defendant REE Automotive Ltd. ("REE Automotive"), originally Soft Wheel Ltd. until its 2019 name change, is a corporation organized under the laws of Israel, with its principal place of business at 10 Aharon Maskin St., Tel-Aviv, Israel, and its headquarters for its U.S. operations in Pflugerville, Texas.

40. Defendant REE Automotive Holding Inc. ("REE Holding") is a corporation organized under the laws of Delaware, with its principal place of business at, upon information and belief, 10 Aharon Maskin St., Tel-Aviv, Israel, and its headquarters for U.S. operations in Pflugerville, Texas. REE Holding is the successor in interest of 10X Capital Venture Acquisition Corp., and a wholly-owned subsidiary of REE Automotive.

41. Defendant REE Automotive USA Inc. ("REE USA") is a corporation organized under the laws of Delaware, with its headquarters and principal place of business in Pflugerville, Texas. REE USA is a whole-owned subsidiary of REE Automotive.

JURISDICTION AND VENUE

42. This action arises under the Defend Trade Secrets Act of 2016, 18 U.S.C. § 1836. This court has subject matter jurisdiction over this case for misappropriation of trade secrets under the Defend Trade Secrets Act of 2016 pursuant to 28 U.S.C. §§ 1331 and because, as described herein, Defendants committed acts in furtherance of their misappropriation in the United States. This Court also has supplemental jurisdiction, pursuant to 28 U.S.C. § 1367, over all state law claims asserted herein because they are related to and form part of the same case or controversy as OSR's federal claim.

43. This Court has general personal jurisdiction over REE USA because, among other reasons, its principal place of business is located in this District.

44. The Court has specific jurisdiction over REE Automotive, REE USA, and REE Holding pursuant to Tex. Civ. Prac. & Rem. Code § 17.042, and consistent with the Due Process Clause of the Fourteenth Amendment, because they "commit[ed] a tort in whole or in part in this state." Specifically, REE USA, REE Automotive, and REE Holding, through their U.S. headquarters, partnerships with Texas-based company, EAVX, and senior employees in the District, have intentionally misappropriated OSR's technology, and have threatened to misappropriate OSR's technology, to fundraise and produce, develop, and market its product, containing misappropriated trade secrets, in the District and to residents of this District.

45. REE publicly stated that "[w]e are excited to call Pflugerville—and Texas—home." REE signed a ten-year lease for this headquarters and "integration center," in which it will develop, market, produce, manufacture, and sell the REE Platform based on trade secrets misappropriated from OSR, including in Texas. From their Texas headquarters and "integration center," REE USA, REE Automotive, and REE Holding, have stated that they will "serve the whole of the U.S." REE intends to quickly begin and scale up production of products embodying OSR's trade secrets at its integration centers, reaching an annual capacity of 600,000 vehicles by 2026, and employing approximately 150 people.

46. REE Automotive, REE Holding, and REE USA are preparing in the District full vehicle prototype testing for customers of REE's products that incorporate OSR's misappropriated trade secrets, in particular the "Proxima Powered by REE," a van for last-mile delivery. REE's primary partner for producing the misappropriated technology is the Texas-based company, EAVX, LLC ("EAVX") a business unit of JB Poindexter & Co., which is also headquartered in

Texas. REE and EAVX worked together to take orders from U.S. customers for the "Proxima Powered by REE." In connection with that partnership, REE Automotive, REE Holding, and REE USA thus each knowingly disclosed OSR's trade secrets to EAVX in the District in order to produce technology based on trade secrets REE misappropriated from OSR.

47. REE Automotive and/or REE USA, and/or REE Holding also entered into an 8-year economic development performance agreement with the Pflugerville Community Development Corp. ("PCDC"), pursuant to which REE obtained a $1 million grant which REE intends to use to develop, produce, market, and sell technology misappropriated from OSR. REE obtained the grant because of technology it misappropriated from OSR. Specifically, PCDC issued a news release stating that the REE headquarters would "expand[] autonomous and electric car technology in the Austin region" and that "REE's research and development capabilities will further define the Austin Region as an EV high-tech manufacturing hub." The PCDC is assisting REE in obtaining skill development funds and other workforce grants to produce the technology based OSR's trade secrets.

48. Moreover, REE USA, REE Automotive, and REE Holding's Director of Financial Planning and Analysis, Global Controller, Assistant Global Controller, and Global Chief Operations Officer, are all based in the District. The Chief Operations Officer, based in Austin, Texas, is responsible for REE Automotive, REE Holding, and REE USA's global operations, manufacturing, and expansion, including, among other things, complex product development and launch, including the launch of REE's products that incorporate OSR's misappropriated trade secrets. REE is also actively recruiting additional employees in the Texas, including product managers, a functional safety engineer, and a senior automotive market research analyst.

49. REE USA, REE Automotive and REE Holding are seeking to avail themselves of the laws of this District and intentionally targeted their conduct at the District. REE has represented that it is targeting Texas for the first deployments of its products, including products based on trade secrets misappropriated from OSR, to avail itself of Texas's laws and incentive plans. Among other things, REE has also announced that the "[t]he Austin region is the perfect choice for bringing to life our . . . platforms at scale, with a highly-skilled tech workforce, well-structured regulatory environment, and entrepreneurial spirit that matches our own" and that REE's "headquarters in Austin, Texas best positions [REE] for growth and rapid expansion," and allow it to "capitalize on the incredible opportunities in the U.S. market." REE stated that this "U.S. presence will allow us to capitalize on the incredible opportunities in the U.S. market and put us closer to our North American-based customers and partners," with which REE is developing, marketing, and selling its products based on OSR's trade secrets. Further, REE is taking advantage of zero emissions mobility grant money from the Texas Commission on Environmental Quality to use to further misappropriate OSR's trade secrets.

50. This Court additionally has specific personal jurisdiction over REE Automotive and REE Holding on the basis of acts in the District by REE USA because they are alter egos of each other and of REE USA, as set forth more fully below.

51. This Court also has specific personal jurisdiction over REE Automotive and REE Holding because REE USA has acted as an agent of REE Automotive and REE Holding in this District, as set forth more fully below.

52. Alternatively, this Court has jurisdiction over REE Automotive pursuant to Rule 4(k) of the Federal Rules of Civil Procedure, to the extent it "is not subject to jurisdiction in any state's courts of general jurisdiction," because exercising jurisdiction is consistent with the United

States Constitution. REE has committed numerous acts in furtherance of its misappropriation in the United States, as described below, including, among other things, selling and marketing the REE Platform incorporating OSR's trade secrets in the United States, hiring employees to support the production and sale of the REE Platform incorporating OSR's trade secrets in the United States, entering into partnerships with U.S.-based companies obtained by using OSR's trade secrets and to develop and sell products based on those trade secrets, and engaging in fundraising using OSR's trade secrets to draw investors. All of these acts were in furtherance of REE's ongoing misappropriation of OSR's trade secrets and the REE Platform's entry into the U.S. market. Jurisdiction in this District over REE Automotive is reasonable, given that, *inter alia*, REE Automotive acts through its agents, REE USA and REE Holding, in this District. The United States and Texas both have a strong interest in enforcing their trade secret laws, as codified in the Defend Trade Secrets Act and the Texas Uniform Trade Secrets Act.

53. Venue is proper in this court pursuant to 28 U.S.C. §§ 1391(b)-(d). A substantial part of the events giving rise to OSR's claims against Defendants have occurred in this district, where REE USA is headquartered. Further, at least REE USA is subject to general jurisdiction in this District, and all Defendants transact business in this District and are subject to jurisdiction in this District under Tex. Civ. Prac. & Rem. Code § 17.042. Venue is thus proper in this District.

FACTUAL ALLEGATIONS

I. OSR CREATES THE EVOLVER

A. The EVOLVER's Revolutionary Centralized Solution for Smart and Self-Driving Cars

54. OSR developed a cutting-edge technology that enables car manufacturers to make smart, safe, autonomous and interconnected vehicles and is itself producing a fully electric vehicle for sale to the public. Beginning in 2011, OSR's founder, CEO, and Chairman, Orit Shifman,

anticipated that the future of the automobile industry would require a central processing unit that could not only control fully autonomous vehicles, but also provide services to end users of vehicles and related industries, including in insurance, fleet management, preventative maintenance, and other day-to-day services. OSR accordingly began work on the "EVOLVER," a revolutionary, advanced hardware and software computing platform that uses AI to act as the "central brain"—as OSR refers to it in marketing materials—for smart and self-driving vehicles by collecting, processing, learning, and making and executing decisions based upon the vast amounts of data collected by a vehicle's various components and processed in this central brain.

55. Most cars today utilize from dozens to over a hundred electronic control units ("ECUs") dedicated to control various electrical systems and subsystems and their associated functions. For example, a car's anti-lock braking system typically has one or more ECUs combined with sensors. Based on data the ECUs receive from the sensors, the ECUs can increase or reduce braking force to prevent the car from skidding. ECUs are typically non-networked or decentralized, meaning they operate independently or in tandem with only a handful of the car's other ECUs generally through a controller area network or "CAN-bus" used to transfer data between sources. Taken together, the ECUs and CAN buses make up, among other components, a car's electric and electronic ("E/E") architecture.

56. Notably, modern cars do not have a single "central computer" that can process, connect, and utilize all of the data processed independently by ECUs. Even some of today's most advanced cars equipped with what is known as advanced driver assistance systems rely upon a decentralized architecture that only connects the relevant ECUs. For example, in a car equipped with automatic emergency braking—that is, a car with sensors to detect objects in front of the car—the sensors are connected to the car's ECU that activates the brakes so that the brakes may

be engaged if the sensors detect an object that the car may collide with, but most of the car's other functions are not connected to the automatic emergency braking system.

57. The EVOLVER represents a brand new approach to E/E architecture. By forgoing reliance on decentralized ECUs incapable of supporting the processing power required for smart and autonomous cars, the EVOLVER's centralized design allows vehicles to more efficiently and intelligently collect, process, and utilize data derived from all of a vehicle's various sensors and data sources, such as external communication devices, video and audio feeds, RADAR, and LIDAR, while still able it to fully interact with the CAN buses and other ECUs of conventional architecture cars.

B. The EVOLVER's Proprietary New Technologies

58. OSR's new approach to powering cars required the development of proprietary new technologies. The resulting developments in the EVOLVER's "central brain" represent a quantum leap in automotive technology. With this centralized and smart system, the EVOLVER, among other things, provides a more advanced solution for smart and fully autonomous—known as "level five"—self-driving cars, and represents advancements in proprietary technologies in a number of disciplines, some of which are described below.

59. *First*, because the EVOLVER is at the center of all of the many sources of input both on the car's interior and exterior, it receives huge amounts of data, which OSR developed proprietary software and hardware methods of collecting, storing, and processing in real-time at high-rates of speed with low latency.

60. *Second*, and perhaps the most revolutionary aspect, is the deep neural AI network that OSR created. OSR developed from the ground up proprietary algorithms and source codes capable of recognizing relationships among this data undetectable to humans, which permit the

EVOLVER to continuously learn and react. For example, with respect to autonomous driving, the EVOLVER constantly takes inputs from video feeds, RADAR, and LIDAR, to recognize objects and detect external risks, e.g., distinguishing between objects, types of terrain, and road edges, across different visibility scenarios—all the while continuously learning from the infinite combinations of scenarios how to better detect risks and obstacles. It can detect pedestrians in a blind spot and calculate their velocity and vector, or whether they are distracted by a smartphone, to predict whether they are at risk and alert the driver or actuate the car's controls to take evasive action. And because the EVOLVER controls the various components of a car, it can adjust them in real time, in ways undetectable to humans, to provide a much more efficient and safer car.

61. The EVOLVER also constantly monitors video and audio feeds within the cabin to provide a smarter and safer driving experience by, among other things, detecting risks in order to alert an inattentive driver or shift between autonomous, semi-autonomous, and non-autonomous driving. For example, the EVOLVER can analyze data from video and camera feeds, as well as countless other sources, to detect the driver's emotions and attention and even medical or other emergencies—including based on her voice, blinking rate, head and eye positioning, and facial expressions, her braking or acceleration pressure, whether her calendar indicates that she is late for a meeting, whether she appears fatigued, whether there are upset children in the car or thousands of other data points that, based on OSR's programming, training, and algorithms, the EVOLVER has learned to be relevant. And the EVOLVER can draw distinctions and reach conclusions from data that can apply either universally to all drivers within the connected system or be tailored to the individual driver, in order to evolve.

62. *Third*, OSR has also adapted the ability of this deep AI neural network with immense data processing and storage power, capable of fully autonomously driving a car, to a host

of what OSR refers to as a "multi-domain brain" for applications across many fields and applications, including, for example:

a. Insurance: The EVOLVER can collect, process, and share vehicle data with insurance companies so that they may in turn provide customized policies and pricing consistent with data relating to an individual's driving characteristics.

b. Predictive Maintenance: The EVOLVER can detect and predict vehicle maintenance issues, for example, predicting that a component will need replacing based on data that is highly driver specific, and even provide over-the-air software updates.

c. Fleet Management: The EVOLVER can manage fleets of vehicles for use in delivery or taxi services, including, for example, tracking the fleet, prioritizing maintenance, optimizing routes based on, among other things, current and historical traffic data and commercial needs.

d. Route Optimization: The EVOLVER can optimize routes based on, among other things, time, the amount of energy expended, speed, preferred driving routes, tolls, and current and historical traffic.

63. Certain of these applications that relate to monetizing data for the purposes of services, insurance, predictive maintenance, and fleet management, are referred to as "Data-as-a-Service." Additional "multi-domain" capabilities include infotainment, digital instrument clusters, and a smart and fully localized AI voice assistant.

64. *Fourth*, the EVOLVER also has advanced cybersecurity capabilities. Because the EVOLVER is networked to various internal (e.g., car systems and sensors) and external (e.g., insurers or other connected vehicles) sources that are potentially vulnerable to attack, it is critical to protect both the data and vehicular control operations from potentially malicious actors. OSR

thereby created methods of network security and encryption to protect the data and control mechanisms. Through years of research concerning these threats and the ways to address them, OSR has created proprietary, multi-layer cybersecurity solutions, consisting of both hardware and software, that provides monitoring and protection of internal and external vehicle communications and data.

65. *Fifth*, OSR spent years adjusting its platform through proprietary methods that would allow original equipment manufacturers (e.g., vehicle manufacturers), or "OEMs," to install the EVOLVER and allow it to function in existing cars. This is a stunning feat that required OSR to tailor the EVOLVER to be adaptable and work with and control an incredibly varied set of components.

66. *Sixth*, the EVOLVER can also be customized for OEMs through a unique set of tools. Using these tools, an OEM can customize EVOLVER to work with their specific vehicle setups (i.e., the OEM's configurations of sensors and vehicle buses), configurations of the communications and data transfer between domains, fleet management needs, remote vehicle control, and additional functionalities. To do this, OSR labored, under non-disclosure agreements, with OEMs in order to best determine the OEMs' needs and create a universal, but adaptable, environment for customization.

67. Because of OSR's shift to centralized architecture for the EVOLVER and the customizability of the EVOLVER, OSR has revolutionized, and will continue to revolutionize, the "time to market" for autonomous and semi-autonomous vehicles in the industry. Indeed, as discussed further herein, the EVOLVER is enabling OSR to bring its own fully electric vehicle based on the latest generation of the EVOLVER, to market in approximately two years.

C. The Commercial Success of OSR's Intensive Labors

68. Creating a computer that supports autonomous control of a car is extremely complicated and time intensive. Because of the EVOLVER's novelty, OSR had to create the necessary software and design hardware from scratch, which required OSR to conduct extensive market research and laboratory testing and studies, and to develop unique engineering and coding know-how, including, among other things, knowledge of unworkable and suboptimal designs for the EVOLVER, through a laborious process of trial and error. The software and hardware must be laboriously tested, revised, and refined to ensure safe, effective, and efficient operation. OSR has spent over a decade developing the EVOLVER by utilizing approximately 150 employees, the vast majority of whom are in research and development, over millions of hours and at a cost of well over $100 million.

69. OSR publicly debuted the EVOLVER, then in its third generation, in the fall of 2017 at the leading international trade show, the IAA.

70. The EVOLVER is now in its sixth generation—with the seventh generation nearly ready for launch—and OSR has been selling versions of its EVOLVERs since 2016. Since then, OSR has been a "tier one" supplier (meaning that it sells components directly to automobile manufacturers) and has worked with some of the largest car manufacturers in the world to embed the EVOLVER into these manufacturers' future vehicles.

71. In September 2019, OSR presented the fourth generation of the EVOLVER at the 2019 IAA trade show both independently and in collaboration with its customer, luxury car maker Jaguar Land Rover, by demonstrating the integration of the EVOLVER in the Jaguar I-PACE sport utility vehicle. At the time, Jaguar Land Rover's chief engineer stated:

> This collaboration with OSR is truly remarkable. . . . We believe coming state-of-art autonomous user services will benefit from this centralised comput[ing] and secure connectivity platform. The very

> practical and extremely fast hands-on approach backed by OSR's vast experience puts us in a prime position for fast collaborative learning and building our strategy going forward.

72. OSR's hard work and investments have paid off. In 2016, before Stauber joined OSR, OSR was valued by a major accounting firm at several billion dollars and since then OSR's valuation has increased substantially.

73. OSR has now leveraged the EVOLVER, including its advances in safety and interconnectivity, and its extensive automotive experience to become an EV OEM itself. OSR plans to have in production in around two years its cutting-edge fully electric vehicle, based on the most recent generation of the EVOLVER. Because OSR's own EV is based on the EVOLVER, it will provide a safe, secure, efficient, and personalized driving experience, while providing uncompromising performance, dynamic drivability, and the thrill of a supercar.

74. The market for creating autonomous cars today is extremely competitive. Many companies around the world are racing to make electric vehicles platforms and vehicles capable of autonomous driving. Cutting the time it may take to develop and build the software and hardware necessary for such a feat would give a company an edge over its competitors. That company could not only bring its product to market sooner but also beat their competitors to limited pools of investor capital.

II. OSR PROTECTS ITS TRADE SECRETS AND OTHER CONFIDENTIAL INFORMATION

75. As a company built on innovation, OSR uses a variety of methods to protect its intellectual property, but chiefly uses trade secrets. Consequently, OSR's trade secrets are crucial to OSR's current and future value. OSR's trade secrets, which represent important technological improvements in the area of autonomous vehicles, derive independent economic value from not

being generally known, and not being readily ascertainable through proper means, by other persons who can obtain economic value from the disclosure or use of the information.

76. Accordingly, and as described in more detail herein, OSR takes, and at all relevant times for this action, employs best-in-class practices and policies to safeguard its trade secrets and the knowledge of how its trade secrets were developed. OSR has adopted these measures and practices to prevent its trade secrets from entering competitors' hands, so that competitors cannot unfairly benefit from OSR's years of investment in the EVOLVER platform. OSR's safeguards primarily consist of three layers: (1) internal cybersecurity policies and practices; (2) physical barriers; and (3) legal protections.

A. Internal Cybersecurity Policies and Practices

77. OSR has developed strict internal cybersecurity policies and procedures to protect its confidential information and trade secrets and prevent unauthorized access or disclosure. Stauber himself commented in an email that neither he nor any of the other employees he had spoken with had ever worked "in a place where the level of security is higher than at OSR."

78. OSR maintains any development-related electronically stored information, including source code, specifications, component lists, and other sensitive materials, on a closed and secured dedicated computer server that is not connected to the internet or to OSR's open internal network. OSR physically locks its terminals in metal cages, which can only be opened by OSR's IT team with proper authorization. Each employee has unique credentials to access this closed system, and employees' degree of access to files on this system is limited to only the materials each employee needs for their respective work tasks. This system prevents the use of external media, such as external hard drives or flash storage drives, to transfer files from this closed system.

79. Material maintained on the closed system, as well as information concerning sensitive customer and marketing information, is not allowed on any laptops or other devices with internet connectivity except on a limited case-by-case basis, such as when such information must be shared with a manufacturing partner. An employee seeking to transfer materials in this manner must first request written permission, and requests undergo multiple levels of review including ultimately by OSR's CEO. Only then, and through a controlled procedure, can such information be transferred outside of the closed system. Employees are forbidden from using external storage devices or email to copy or transfer any information from OSR devices. To the extent any such information is then transmitted outside of OSR, it is pursuant to strict guidelines and conditions, such as pursuant to a non-disclosure agreement.

80. For the entirety of Stauber's employment at OSR, the vast majority of OSR's employees and engineers shared a single dedicated laptop, for use only on business trips or presentations outside of the office, which is password protected and encrypted. To the extent internal OSR information is necessary for such a trip, this is the only device to which any such information is loaded. Any other laptops are provided to select managers, such as Stauber, solely for the purpose of accessing company email, which employees are prohibited from using to transfer sensitive or development materials. Employees are prohibited from downloading or saving any development or customer-related information to these laptops. Employees have separate locked computers to be used for development purposes.

81. Additionally, OSR information may only be deleted from OSR's servers with specific approval and only by OSR's internal information technology team.

B. Physical Protections

82. OSR also restricts access to its trade secrets through physical barriers to access.

83. OSR maintains strict control over physical access to its offices. In order to enter OSR's offices, employees must pass through two layers of security: a turnstile and an electric locked door, both of which restrict access to employees with a secure near-field-communication ("NFC") tag.

84. Visitors may only access OSR's offices with prior written approval from OSR management. Before entering, they must provide a personal identification card to building security in order to receive an NFC tag. Visitors may not access areas of the office where product development occurs and are generally prohibited from carrying smartphones on the premises.

C. Legal Protections, Training and Oversight

85. OSR also requires all employees, including Stauber, to enter into employment agreements at the commencement of their employment that incorporate a "Secrecy, Non-Competition and Proprietary Information Agreement" (the "Secrecy Agreement").

86. The Secrecy Agreement defines "Confidential Information" broadly to include, among other things:

> any and all information concerning the business and affairs of [OSR], product specifications, data, know-how, compositions, processes, formulas, methods, designs, samples, inventions and ideas, technology in various stages of development, past, current and planned development or experimental work, current and planned distribution methods and processes, customer lists, current and anticipated customer requirements, price lists, market studies, business plans, hardware architecture, - structure and - technology and related hardware know-how, hardware inventions, hardware discoveries, hardware designs, hardware developments methods and - information, computer software and programs (including object code and source code), computer software and database technologies, systems, structures and architectures (and related processes, algorithms, compositions, improvements, know-how, inventions, discoveries, concepts, ideas, designs, developments, methods and information) of the Employer, and any other information, however documented or not documented of the Companies . . . .

87. As part of the Secrecy Agreement, employees acknowledge the value of the Confidential Information and agree not to use, copy, or disclose it except as required for carrying out their duties or as required by law.

88. The Secrecy Agreement also provides that the obligations pertaining to nondisclosure of Confidential Information "are perpetual, and shall survive the termination of [the employee's] Employment with [OSR]."

89. Pursuant to the Secrecy Agreement, any Confidential Information or Inventions (as defined therein) are and shall remain the exclusive property of OSR and any ideas, inventions, trade secrets, or other developments that an employee created or conceived during employment with OSR is considered a "work made for hire" under copyright law and/or assigned to OSR.

90. Further, upon termination of employment, employees are required to return to OSR all OSR written and tangible material relating to OSR's business and may not retain copies of any materials containing Confidential Information.

91. The Secrecy Agreement also contains a non-compete provision to minimize the risk that OSR's valuable trade secrets are acquired by competitors from former employees, which prohibits OSR employees from joining, or soliciting other employees to join, competitors as employees, officers, or consultants for 24 months after termination of their employment at OSR.

92. In addition to entering into the Secrecy Agreement, employees also receive training on security procedures at the commencement of and periodically throughout their employment. All employees are trained in OSR's cybersecurity policies through internal company tutorials, and managers are trained to monitor employee compliance with OSR's policies.

93. OSR's security procedures are updated regularly and then communicated to employees. OSR also regularly sends employees reminders of its security policies. Further, OSR

monitors for breaches of its procedures and, where a breach is detected, OSR notifies involved employees and takes appropriate remedial actions to prevent further breaches.

III. REE MISAPPROPRIATES OSR'S TRADE SECRETS TO DEVELOP A COMPETING "CENTRAL BRAIN" FOR CARS

A. REE's Technology Prior to Misappropriating the Trade Secrets

94. Until recently, the REE Platform was rudimentary and largely mechanical with no centralized ECU platform, AI functionality, or multidimensional data processing capabilities. There was no prior indication that REE was developing such a platform or was even in the business of building one.

95. REE was founded in 2011 as "SoftWheel" by an Israeli farmer, Gilad Wolf, and a partner, to market and sell a form of in-wheel suspension for wheelchairs that Wolf had invented in 2008 after he broke his pelvis. Although REE's current CEO, Daniel Barel, often refers to himself as a "co-founder" of SoftWheel, he apparently only joined SoftWheel in 2013 when he became its CEO. Prior to that, Barel founded a now-defunct social-network app for dog owners called *Wooof* while working in management consulting.

96. Over time, SoftWheel also built a bicycle with its in-wheel suspension device, but SoftWheel's product was entirely mechanical; it did not relate to automobiles at all, much less self-driving cars. However, with Barel at the helm, SoftWheel sought to take advantage of the flood of investment money flowing to the electric and autonomous vehicle markets in the United States, particularly through SPACs, which rose to prominence in 2019 as a rapid mechanism for private companies to become public while making minimal disclosures.

97. In June 2019, at an Israeli transportation trade show, SoftWheel publicly debuted itself as REE, formally changing its name in December of that year, and announced that it was in the process of developing the REE Platform. Like SoftWheel's product, the REE Platform was

only an in-wheel system. It consisted of the "REEboard"—a flat chassis referred to in the automobile industry as a "skateboard" and conceived of at least as early as 2002 by General Motors—and the "REEcorners"—a system of housing next to each of the four wheels the car's major components, including the brakes, motors, suspension, and drive train. Consistent with SoftWheel's prior products, the REE Platform was largely mechanical in nature.

98. Nothing in REE's June 2019 presentation suggested that the REE Platform included, or that REE intended to develop, a centralized AI control unit, or anything to do with advanced computerization, data processing and storage capabilities, or cyber security. REE's emphasis on distributing vehicle components, such as motors, steering, suspension, drivetrain, and electronics, separately into each of the four wheels of a vehicle is the opposite of the EVOLVER—a single central system for managing these functions in whatever configuration a vehicle manufacturer designs. In fact, REE touted that the primary advantage of the REE Platform *was* its decentralization, due to its purported space-saving features and ability to swap out wheels when components broke down.

99. That REE was focused on its mechanical, in-wheel system, as opposed to an advanced, computerized central control system with AI is epitomized by Barel's statements at REE's June 2019 debut. In a consciously Apple-launch styled presentation, Barel paced across a stage commenting on the state of the automotive industry and expressing shock and amazement at other companies' AI and autonomous driving technology:

> And autonomous—oh boy autonomous! Just ***go out here*** and see—I mean today we've got words like LIDARs, RADARs, sensing, mapping. I've read something that says that today, a car is actually smarter than a jet plane. I still can't get over the fact that we literally have lasers coming out of cars!

(emphasis added). By the time of Barel's presentation, concepts like LIDAR, RADAR, sensing, and mapping were basic and fundamental to the automobile industry. Given the complexities of,

for example, traffic congestion and set routes, these cars *must* be smarter than a jet plane. But to REE in June 2019, it was all a mysterious, if attractive, world apart.

100. Developing central processing units, like the EVOLVER platform, requires significant experience and investment of time and money in, among other things, the use of sensors (to collect and deliver data to the central processor), network technologies, machine learning, and AI. Indeed, even building and training a neural network with machine learning requires iterative development—for example, feeding the system a vast number of inputs and then correcting the conclusions it draws—that, by its nature, is iterative and necessitated enormous amounts of time to develop. REE did not demonstrate that it had any of this necessary experience or suggest in any way that this was an area it was exploring.

101. Moreover, REE demonstrated that it still had a long way to go before bringing even its own mechanical prototype REE Platform to market, which had then progressed no further than a plastic miniaturized prototype and primitive 3D sketches as shown in the images below:[2]

[2] *See* REE, *Daniel Barel at EcoMotion June 2019*, YOUTUBE (Sept. 5, 2019), https://youtu.be/BBIlrD-SqUA.

102. Following its June 2019 presentation, and throughout the remainder of 2019, REE continuously emphasized the REE Platform's "decentralized ECU network," meaning that the components are distributed across the vehicle, rather than centralized, as in OSR's EVOLVER. For example, the below screenshot from a video posted by REE on YouTube in September 2019, emphasizes the decentralized nature of the REE Platform:[3]

[3] *See* REE, *The Future of Electric Mobility*, YOUTUBE (Sept. 4, 2019), https://youtu.be/RnbSnVPFSNg.

103. Around the same time, in September 2019, REE presented at the 2019 IAA trade show in Germany, the same trade show where OSR showcased the EVOLVER already at work inside of a Jaguar I-PACE. In advance of the show, REE issued a press release on September 11, 2019, describing REE and the REE Platform by emphasizing its modular, decentralized approach:

> The company's architecture solution integrates the motors, steering, suspension, drivetrain, sensing, brakes, thermal systems, and power management into the wheel. By integrating all drive components into the wheel, REE offers a completely flat modular skateboard chassis that allows optimal design flexibility and multiple body configurations on a single platform. . . . .

104. Thus, based on REE's own descriptions of the REE Platform in 2019, the EVOLVER and the prototype REE Platform plainly had little in common: the EVOLVER was a centralized computing platform designed to become the "brain" inside of the latest versions of existing and future vehicle models, whereas the prototype REE Platform was a largely mechanical, modular electric vehicle intended to replace the traditional chassis with one where the engine or motors, as well as other components, were placed beside the wheels instead of in between them. The REE Platform also had none of the EVOLVER's advanced features, like AI or multidimensional data processing and analysis.

B. REE Finds Itself to be a Bit Player in a Crowded Field

105. In contrast to REE's early-stage prototype "REE Platform," several competitors of REE were already further along in the development process with superior competing products.

106. The concept for a configurable chassis that REE is selling is as old as the automobile itself. In the early 1900s, Rolls Royce produced a "rolling chassis" containing the car's mechanical elements which would then be sent to bespoke coachbuilders who would attach the bodywork according to customer specifications. This only changed in the early 1920s when

mass-market car makers began building the coach in-house. And, in 2017, Rolls Royce once again returned to coachbuilding, allowing customers to design coaches on top of their universal chassis.

107. More recently, the configurable chassis has been widely adopted by more advanced competitors in the EV space. In or around late-2017, the Swiss Company, Rinspeed AG, introduced the "Rinspeed Snap" which incorporates an "intelligent chassis," called a "skateboard," similar to the REEboard, with decentralized components in "pods," similar to REE's decentralized REEcorners. Canoo, another REE competitor, produces a configurable central "chassis" or "skateboard," called a "Multi-Purpose Platform," with "modular" expandability, similar to the REEcorner's functionality, which is used in vehicles that are available for pre-order. Rivian Automotive, through a partnership with Amazon, has built electric delivery vans, already in production and testing, on a skateboard chassis with two dual-motor units mounted on each axle. And during the Tokyo Olympics in summer of 2021, Toyota showcased its e-Palette vehicle, an autonomous shuttle built on a skateboard chassis.

108. REE's decision to locate components like the motor, powertrain, brakes, steering at the wheel of a vehicle (as part of the REEcorner) is similarly old-hat. In-wheel motors were first developed in the 19th century and used in early electric cars. Multiple major automobile manufacturers have developed in-wheel electric motor technology that also incorporates steering and brakes. For example, Hyundai was researching in-wheel motor systems, including suspension, steering, electric motor, friction brake, and wheel, as early as 2010, Hyundai demonstrated a concept car using its in-wheel technology in 2015, years before REE revealed its prototype REE Platform. Nissan's BladeGlider vehicle, demonstrated in 2013 at the Tokyo Motor Show, also utilized in-wheel motors with independent wheel control.

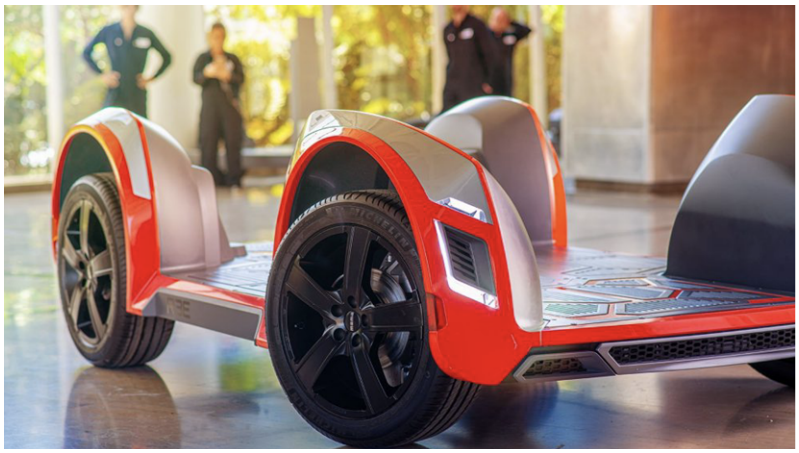
109. More recently, Protean Electric—founded in 2009 and focused specifically on in-wheel motor technology—developed in-wheel motors for use in EVs, which include "integrated power electronics and digital control, packaged with a compatible friction brake." And in July 2019, only a month after REE's public launch of its prototype, Protean announced its "Protean360+" corner module, which is used in all four corners of a vehicle and integrates "advanced powertrain, steering, and suspension technologies."

110. More generally, most OEMs are already manufacturing and selling EVs and have the capital and experience to build their own platforms. Without unique technology, competition from OEMs would likely prove devastating to REE's ability to capture its target market.

111. REE's lack of differentiation from its competitors was highlighted at a 2021 Mobility Disruption Conference, where REE was asked by an analyst "[h]ow would you compare yourself versus say Canoo . . . there's a lot of other skateboards out there." REE struggled to offer a response other than the fact that REE was focused on the commercial vehicle market (which others, like Rivian and Canoo, in fact, are also focused on). Barel even acknowledged the existence of competitors with similar products, noting that "there are a few players out there, some major OEMs," but again falsely claimed only that they "do not exist in specific market commercial businesses."

112. The extent to which REE's technology was eclipsed by competitors would have been brought into vibrant focus at the 2019 IAA conference where REE was surrounded by direct and indirect competitors with far more advanced products. OSR and Jaguar's I-PACE collaboration too was prominently displayed.

113. For example, here is the miniaturized prototype that REE displayed at the 2019 IAA show:



114. And here is an image of the Rinspeed SNAP's platform at the same trade show but as a more advanced, completed model:

115. Similarly, Canoo's working model, debuted the same month:

As of July 2022, Canoo had an agreement with Walmart for thousands of electric delivery vehicles, and in December 2022, Canoo delivered its Light Tactical Vehicle truck to the US Army for analysis and demonstration.

116. In contrast to REE, OSR already had a fully functional version of the EVOLVER installed in a Jaguar I-PACE vehicle, as shown at the 2019 IAA.[4]

[4] *See* OSR Enterprises AG, *OSR Enterprises AG and Jaguar Land Rover*, YOUTUBE (Dec. 19, 2019), https://youtu.be/vN_XSYtJ0-g.

C. REE and Stauber Steal OSR's Trade Secrets

117. REE believed that it needed at least $500 million in investment to bring a product to market. But with this crowded field of more advanced competitors, REE had no way of differentiating itself to investors. Accordingly, REE devised a plan to quickly transform itself into the type of cutting-edge technology company it had always dreamed of becoming—not by developing the technology by itself, which would take far too long to avail itself of the SPAC fad, but by stealing it from a company already established as a leader in the industry: OSR.

118. REE began by setting out to systematically recruit as many OSR research and development ("R&D") employees as it could, starting at the top. For example, in July 2019, shortly after its disappointing launch, REE unsuccessfully attempted to recruit OSR R&D's General Manager of Research and Development by contacting him on LinkedIn to "discuss potential opportunities."

119. In the Fall of 2019, however, unbeknownst to OSR, REE succeeded in recruiting Ohad Stauber, then the Vice President and Head of Research and Development at OSR R&D. Stauber had joined OSR in January 2017 as a mid-level Architecture Team Manager, a position he

held for about a year before OSR R&D gave him the opportunity to serve as Head of Research and Development. Prior to working at OSR, Stauber worked at Intel on 3D mapping and had no experience in the automotive industry. Stauber was able to learn from OSR's substantial investment of time and money and the years of work since 2011 that had gone into building the EVOLVER. By the time Stauber left OSR, he had been given high-level access to OSR's most valuable and secret technology.

120. Stauber's two years of experience in the automotive industry (obtained at OSR) and 3D mapping ability was not what had attracted REE to him. It was Stauber's knowledge of and access to OSR's technology, gained by virtue his senior position and OSR's trust in him, which REE wanted him to disclose and use to recreate the EVOLVER for REE. The problem was that Stauber could not do this on his own and from his knowledge and memory, because the EVOLVER had been developed through the work of approximately 150 mostly research and development employees across a host of disciplines over many years, starting years before Stauber joined OSR.

121. As REE knew, Stauber had significant access to OSR's trade secrets, including the designs of certain EVOLVER products, software implementations of various EVOLVER applications, software tools for OEMs, cybersecurity analyses, designs, and implementations, AI algorithms, and configurations of vehicle sensors and communications channels, as well as knowledge of unworkable or suboptimal designs for the EVOLVER and its code, hardware, and applications. To protect this knowledge and training, OSR had required Stauber to enter into the Secrecy and Non-Compete Agreements, described above, and ensured that he was aware of OSR's strict policies to protect its confidential information and trade secrets, including its specific prohibition on copying OSR information to personal devices.

122. In order to attempt to recreate the EVOLVER for REE as quickly as it wanted him to, Stauber hatched a plan to steal OSR's proprietary data for REE by using a laptop computer issued to him by OSR (the "Stauber Laptop").

123. On September 5, 2019, several days before the 2019 IAA trade show that was attended by both REE and OSR, Stauber researched REE and its developments on the Stauber Laptop. Stauber had no legitimate reason related to his work at OSR to examine REE, whose prototype product was then completely different from OSR's EVOLVER. At that time, Stauber had almost certainly engaged in employment discussions with REE—which had long been targeting OSR R&D's employees—notwithstanding that Stauber's employment agreement prevented him from working there for two years after leaving employment at OSR.

124. Three days later, on September 8, 2019, Stauber arrived at the IAA trade show in Frankfurt, Germany, at OSR's expense. REE and Stauber knew that at the IAA trade show, certain of OSR's proprietary data would, for a short time, be outside of the closed system and relatively unsecure. In order to present at the trade show, OSR had its specific authorized employees, prior to Stauber's arrival, copy onto a designated laptop specifically for the IAA trade show confidential source code and other proprietary files for OSR's platform into a folder called IAA2019. Stauber used that opportunity, when those files were relatively unsecure and outside of the closed network, to copy OSR's files onto an external drive. Stauber had no legitimate reason related to his role at the trade show or otherwise, to copy OSR's files to an external drive. In fact, as discussed above, OSR's policies strictly prohibited Stauber from doing so.

125. Demonstrative of his malicious intent, the drive that Stauber had himself brought to the trade show was particularly large, with a four Terabyte storage capacity, capable of storing, for example 2,000 hours' worth of movies—or enormous amounts of OSR's proprietary data.

126. OSR was able to determine that Stauber connected external hard drives to the Stauber Laptop on numerous occasions, including on September 9 and 11, 2019 even though Stauber was prohibited from storing OSR's sensitive or development materials on that laptop and from using external storage devices. Stauber had copied to these external hard drives—in violation of his contractual agreement, OSR's policies, and the law—over 100,000 of OSR's proprietary files totaling more than 20 gigabytes. As explained in further detail below, these files included, but were not limited to, OSR's proprietary source code packages for the EVOLVER platform contained in the folder "IAA2019," system drawings and blueprints, schematics, data sheets, market research, technical analyses, interface designs, and applications of AI algorithms (the "Stolen Files").

127. Only a few weeks after returning from the trade show, on November 4, 2019, Stauber visited REE's offices, using the Stauber Laptop to determine his driving route. Two days later, on November 6, Stauber gave notice that he was resigning from OSR; his last day at OSR's offices was November 25.

128. OSR determined that Stauber had improperly connected external hard drives to the Stauber Laptop on September 15, October 7, and November 24, 2019, the day before Stauber's last day at OSR's offices. Stauber had no legitimate reason to connect external drives to the Stauber Laptop. And when Stauber returned the Stauber Laptop to its owner, OSR, he did not return to OSR any hard drives containing the Stolen Files, in breach of the Secrecy Agreement.

129. Prior to his departure, Stauber also deleted gigabytes of files from the Stauber Laptop—files likely first copied to external drives that Stauber still has. In part, Stauber sought to cover his tracks by deleting copies of the Stolen Files, which he knew he was prohibited from having copies of. Among the files that Stauber deleted was a folder containing proprietary work

developed by a colleague at OSR, which Stauber had no legitimate reason to have had on his laptop in the first place.

130. Even more sinisterly, Stauber sought to sabotage OSR for the benefit of his new employer. Stauber deleted development files that, in violation of OSR's policies, he had worked on only on his laptop, and were not contained elsewhere. Stauber would have no personal reason to sabotage OSR except that it benefitted REE.

131. Additionally, in the course of its investigation, OSR learned that, while at OSR, Stauber had violated company policy by using his personal phone to take photographs of internal prototypes of circuit boards, hardware configurations, and physical architecture. Stauber never returned these photographs either. However, because Stauber had successfully deleted many files from the Stauber Laptop, OSR has so far been unable to uncover the full scope of Stauber's theft.

132. Stauber began working at REE on December 20, 2019, in direct violation of his non-compete agreement, and in the exact same position he had held at OSR.

D. REE Recruits Additional Employees Despite OSR's Demand Letter

133. In January 2020, OSR, through counsel, sent a letter to Barel, REE's CEO. In that letter, OSR informed Barel that Stauber had violated various terms of his employment contract with OSR and had stolen OSR's files.

134. REE was thus fully aware, since at least January 2020, that Stauber had brought with him the Stolen Files and trade secrets. Rather than take corrective action, however, REE brazenly redoubled its efforts to steal from OSR and exploit OSR's trade secrets for its own benefit.

135. REE knew, or quickly learned that, even with the benefit of the vast treasure trove of Stolen Files, Stauber alone still could not recreate or utilize OSR's technology without the technical know-how of additional OSR employees. Accordingly, knowing that OSR's employees,

like Stauber, were contractually prohibited from working at REE, REE aggressively recruited other OSR employees in order to complete their scheme to misappropriate OSR's trade secrets. REE was successful in recruiting at least eight additional OSR employees, many over the course of just a few months.

136. Specifically, Ron Lupovici, OSR's hardware leader, was recruited by REE as a hardware manager in mid-2020. Alexander Teryohin, formerly OSR's digital signal processing and hardware engineer, was recruited by REE as a hardware engineer in January 2020. Dmitri Gurevich, formerly OSR's senior mechanical engineer, was recruited by REE as a thermal hardware engineer in January 2020. Arik Ben Shitrit, formerly an OSR hardware technician, was also recruited as a practical engineer and hardware technician by REE in June 2021. And REE recruited at least four real-time embedded software engineers—programmers who work on embedding source code within hardware, which is particularly difficult to recreate without the personnel: Denis Rodman, Alex Liberman, Yossi Varman, and Eli Sidi. Further, several more of OSR's other employees have reported receiving employment overtures from REE through LinkedIn.

137. As explained further herein, these employees and Stauber (together, the "Former Employees") were trained in the automotive field solely by OSR and had access to OSR's proprietary developments and trade secrets and each of them was subject to the Secrecy Agreements prohibiting them from working at REE or disclosing OSR's confidential information. None of the Former Employees had any background in the automotive industry prior to working at OSR—all of their industry-specific knowledge and experience was the result of the training they received at OSR.

IV. REE USES OSR'S TRADE SECRETS AND TERMINOLOGY TO TRANSFORM ITS BUSINESS MODELS

A. REE Suddenly Introduces OSR's Trade Secrets Into the REE Platform

138. Over the course of 2020, consistent with its presentations and marketing materials in 2019, REE's marketing materials continued to emphasize the REE Platform's use of a decentralized ECU network approach relying on a REEboard and REEcorners, in which the REEcorners functioned independently of each other with no mechanical connections between any of the wheels.

139. Then, in early 2021—a little over a year after REE hired Stauber and other OSR employees—the REE Platform changed dramatically.

140. While REE had previously touted the advantages of its decentralized nature and mechanics as its key competitive advantage, it was now advertising that it had an advanced centralized computer processing control system called the "REEcenter." Not only had REE suddenly shifted from a rudimentary mechanical system of storing car components in the wheel to save space into highly-advanced central computing system, it also was touting incredibly advanced capabilities in the areas of AI, data processing and storage, and autonomous driving. And it was advertising multi-dimensional applications that precisely mirrored those of OSR's EVOLVER, including, explicitly fleet management, route optimization, insurance, and preventative maintenance. (*See supra* at ¶ 62.)

141. REE's investment advisor, Cowen & Co. ("Cowen"), issued an analyst report in August 2021 that marked REE's stock as likely to "outperform." In its report explaining its rating, Cowen expressly stated that "REE's software services integrating neural net AI technology enables predictive maintenance to further lower costs" and noted that REE's model relies, *inter alia*, on sales of "integrated motors, ECUs and *related software*, which are higher margin than traditional

EV related component companies" (emphasis added). Cowen also noted that REE "pitches itself to be a tech company" with higher margins compared to OEMs in the industry and highlighted REE's so-called "X-by-wire" technology (described more fully below), a technology stolen from OSR, as a feature that makes REE's platform "future proof" and differentiated in the EV market. Additionally, according to Cowen, part of REE's "value proposition" is its "smart technology through its advanced data collection and preventive maintenance A,I [sic]." Thus, it is clear that a significant part of the value of REE's stock, and REE itself, derives from the technology it stole from OSR.

142. REE's sudden and new claimed capabilities were announced by none other than Stauber himself. In a video REE posted to YouTube on May 19, 2021, Stauber described the REEcenter as the "central brain" of the REE Platform connecting the REEcorner ECUs—even adopting OSR's precise marketing terminology. (*See infra* at ¶ 150.) REE's descriptions precisely mirrored the capabilities of the EVOLVER, which, as described further herein, were stolen from OSR.

1. REE's Advanced AI "Central Brain" with "Autonomous Drive" Capabilities

143. Stauber explained that the REEcenter would be an autonomous-ready AI-powered centralized platform:

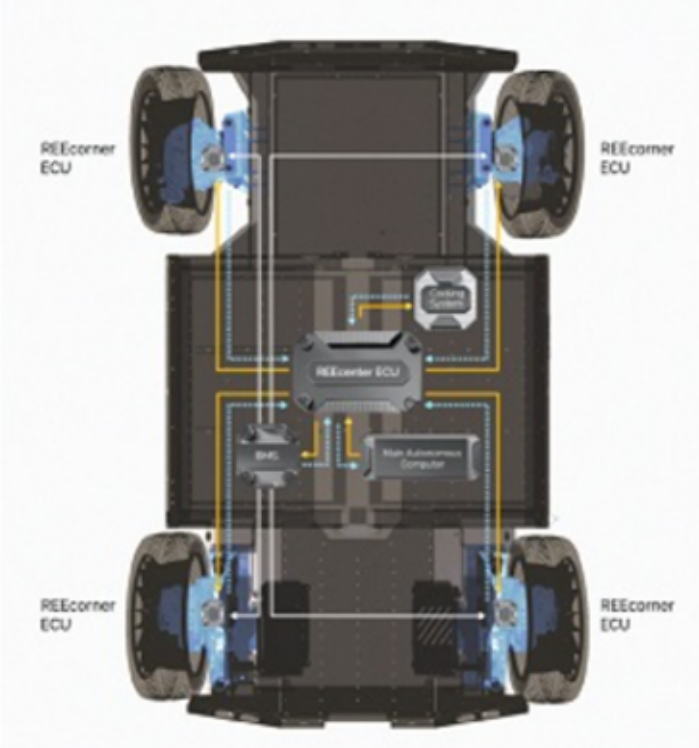
> responsible for all [of the REE Platform's] high-level decision making and vehicle dynamics decisions. For example, upon making a turn at high speed, the REEcenter will decide what is the exact steering angle of each wheel, what is the exact torque and breaking power of each wheel, and whether we should activate torque vectoring capabilities.

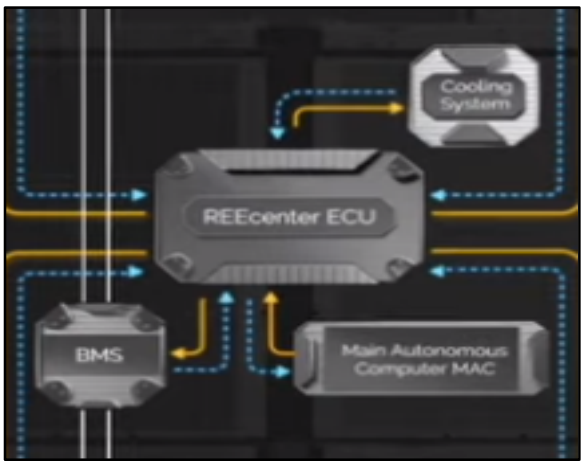
144. This description (publicized by REE less than two years after it had emphasized its decentralized architecture) was echoed in one presentation that called the REEcenter the "primary

brain of the platform, controlling all corner level functions" and stated that the REE Platform would suddenly have:

- "Autonomous Drive" capabilities, described as "REE technology designed to manage all vehicle dynamics functions, allowing for smoother and safer autonomous driving and faster time to market," and could
- "[F]acilitate [Advanced driver-assistance systems] Technology implementation through to Level 5," which refers to fully-autonomous driving.

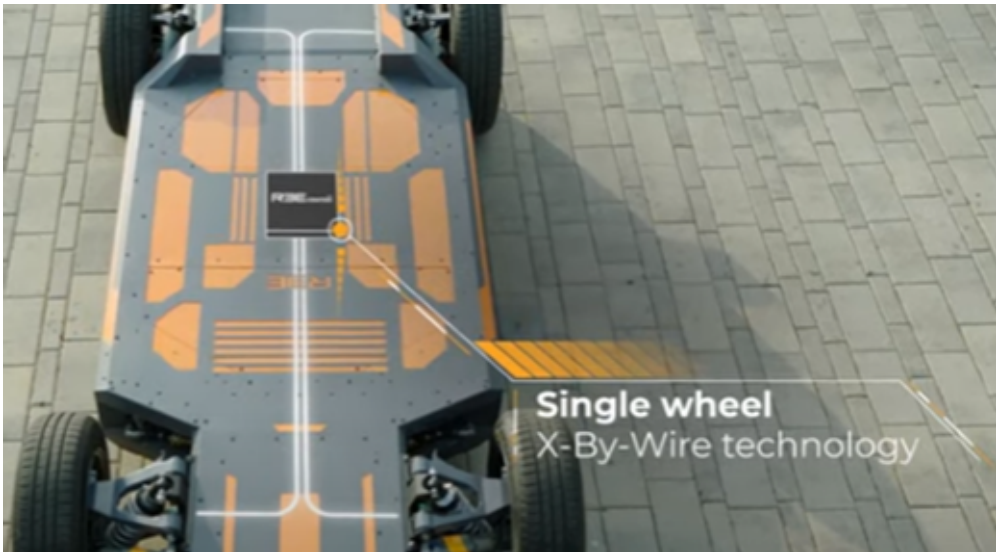
145. And REE's investor presentations marketing materials suddenly showed a REEcenter in the middle of its flat chassis with a "Main Autonomous Computer":



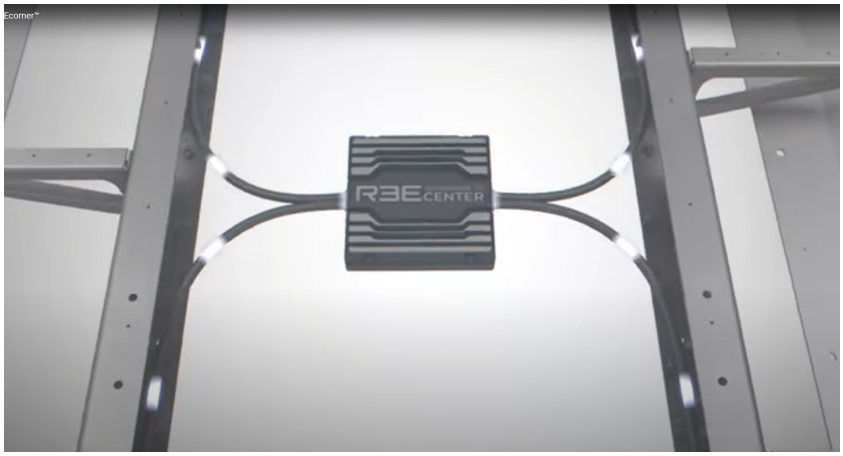


146. Thus, while prior to stealing OSR's trade secrets, the REE Platform was incapable of any high-level decision-making, now it was performing the type of advanced data analytics and real-time decision making that OSR had spent years developing for the EVOLVER, and was even capable of autonomous driving. (*See supra* at Part I.B.)

147. A few months later, at the end of 2021, REE announced its "Leopard" vehicle, which it describes as an "autonomous last-mile delivery concept vehicle." The Leopard, like REE's other announced vehicles, includes the REEcenter in the middle of the platform.



148. REE has also recently promoted the REEcenter as part of its "P7 EV platform" (see image below), for commercial trucks and vans:[5]



REE is integrating the P7 EV platform into a product it is developing with Texas-based EAVX, called "Proxima Powered by REE." In November 2022, REE announced that it had conducted over the past few months "successful demonstration events" of Proxima Powered by REE in the US which led to "orders for Proxima Powered by REE from several leading US fleets." REE further noted that it had commenced assembly of its P7 EV platform chassis "upon which, together with [Texas-based] EAVX, it intends to deliver Proxima Powered by REE test fleets as a fully homologated vehicle for use on public roads in the US."

2. Data Collection, Processing, and Storage

149. In the May 2021 video, Stauber also stated that the REE Platform is "designed to accommodate sensors for deep and robust data gathering allowing for storage, analytics, and decision-making processes." These high-capacity data gathering, storage, and analytics are a key competitive advantage of the EVOLVER. For example, an OSR press release from years earlier in 2017 stated that:

[5] *See* REE, *P7 EV platform starting from the REEcorner™*, YOUTUBE (Mar. 8, 2022), https://youtu.be/iAW8UwyY9O4.

> The EVOLVER powers in-vehicle Machine Learning and AI based on massive amounts of data related not only to the driver and passengers in the vehicle itself but also to its surroundings. . . . The central unit is not only more powerful, but also has significant cost advantages and is energy-efficient. "Evolver . . . outperforms competitors in terms of speed, in data processing power . . . . A common configuration of the Evolver-platform has a better degree of capacity usage for deep-learning applications and that at a lower power consumption.

And elsewhere OSR repeatedly referred in marketing to the EVOLVER as "Artificial Intelligence for Real-Time In-Car Massive Data Processing."

3. AI-Enabled Multi-Domain, Data-as-a-Service Capabilities

150. Stauber also announced that the REE Platform was now suddenly capable of using data gathering, storage, and AI decision-making for what REE was referring to as "multi-dimensional" data as a service capabilities:

> [F]or multi-dimensional data as a service capabilities with our proprietary AI driven software we plan to offer preventive maintenance, predicting problems before they have taken place and resolving them across a fleet. The smart technology can offer future services such as fleet management, route optimization, insurance, and maintenance as a service."[6]

151. These directly paralleled OSR's "multi-domain" Data-as-a-Service capabilities, and, too similar to the EVOLVER's offerings to be mere coincidence, included fleet management, route optimization, insurance, and preventative maintenance. (*See supra* at Part I.B.)

4. Cybersecurity

152. REE also suddenly began touting its "cybersecurity" capabilities. In a 2021 proxy statement filed with the SEC, REE promoted its work to "further explore" the potential of the REE Platform in the area of cybersecurity and had developed proprietary protocols to that end. But

[6] *See* REE, *Ohad Stauber, VP R&D, REE Automotive*, YOUTUBE (May 19, 2021), https://youtu.be/1E-7PYL4i0E.

even as of fall 2020, REE had stated that it was focused on "one layer" of the automotive industry—as a "platform" provider that develops the vehicle chassis, *not* as a data provider that supplies communication, cloud computing, and cybersecurity for electric vehicles. Thus, REE's new focus in 2021 on cybersecurity, which is one of the EVOLVER's key strengths and a focus of OSR's research and development, also tracks its incorporation of additional OSR Trade Secrets.

153. REE also announced that its platform had suddenly developed the ability to block malware attacks (i.e., cybersecurity threats) "via proprietary protocols." Cybersecurity is a core competency of OSR's EVOLVER. As OSR's marketing has explained:

> We at OSR realized the inherent vulnerabilities in distributed architecture over CAN bus from the get-go. We knew from the very beginning that variants of in-vehicle firewalls, deep packet inspection and software solutions alone are not enough. Providing cyber protection for the vehicle requires the creation of a combined hardware and software solution to protect the vehicle's both internal and external communications.

154. As with the other advancements, cybersecurity is incredibly time-intensive and costly to develop, requiring years of research and development to make the system effective and safe.

155. Stauber's description of the REEcenter is strikingly—and not coincidentally—similar to the EVOLVER, including his reference to the REEcenter as a "central brain" for the car, exactly as OSR had long referred to the EVOLVER, including for years before Stauber joined OSR.

B. The REEcenter Could Not Be Developed Without OSR's Trade Secrets

156. That REE could have developed these capabilities on its own in the approximately one year between Stauber joining REE and REE announcing the REEcenter is inconceivable. And indeed, as described *infra* at ¶ 260, in subsequent communications among counsel, REE implicitly

confirmed that it had not developed the REEcenter until after Stauber joined REE, in late December 2019.

157. Among other things, many of these functions require significant money, labor, and time to develop, time that cannot be meaningfully decreased, because these functions require extensive amounts of data collection and iterative development involving a tedious and laborious trial and error process. For example, creating an AI capable of advanced decision making or multi-domain capabilities involves time-intensive machine learning in which the neural network is "taught" by feeding it massive amounts of data from which the AI sorts through and draws conclusions, which then must be continuously analyzed, corrected and adjusted. And in the high-speed application of automotive driving where lives are at stake, there is zero tolerance for mistakes, making development time even more difficult to reduce.

158. OSR expended vast resources over nearly a decade developing the software and hardware to create the EVOLVER, which involved not only writing the software code and building the hardware incorporating it, but also a tremendous investment of time and money in research; development of the concept and system architecture; testing, refining and debugging its applications; and machine learning.

159. What's more, when REE hired Stauber it only had 35 employees in total, including not just engineers, but human resources, recruitment, and business development. This is in stark contrast to OSR's approximately 150 employees, the vast majority of whom were in research and development, who had been working on the EVOLVER for years.

160. Thus, REE seemingly required only a fraction of EVOLVER's development time to implement and mirror many of EVOLVER's most high-tech functions. The only explanation

for this severely truncated development timeline is that REE was able to exploit OSR's trade secrets to expedite REEcenter's development.

C. REE Adopts OSR's Marketing Terminology

161. Reflecting REE's brazenness and lack of independent thinking, REE not only copied OSR's trade secrets but also expressly adopted its marketing terminology.

162. For example, at the 2019 IAA trade show, OSR prominently featured the phrase "Freedom to Create" in its presentation materials and booth, as pictured here:

By mid-2020, REE co-opted this phrase, stating in a press release that the REE Platform too offers customers "freedom to create":

> REE has developed the next generation EV platform . . . providing customers ***full design freedom to create*** the broadest range of EV, and Autonomous vehicles for current and future applications, including last mile delivery, MaaS, light to heavy duty EV logistics and robo taxis. . . . The wide array of REE's modular platforms offer ***unprecedented design freedom to create***.

Elsewhere REE has repeatedly referred to "freedom to design," including as demonstrated below:

163. OSR also described EVOLVER as a "brain," "one brain," "single brain," and "central brain," since it first formally presented EVOLVER in 2017.[7] The following marketing materials are examples:

[8]

[7] *See* New Mobility World, *New Mobility World 2019 – Media Night Panel: Digitization of the Mobility Sector*, YOUTUBE (Oct. 6, 2017), https://www.youtube.com/watch?v=2S-7wdNyr-o.

[8] *See Das Auto der Zukunft braucht ein zentrales Gehirn – Interview Orit Shifman (OSR Enterprises)* [The Car of the Future Needs a Central Brain - Interview Orit Shifman (OSR Enterprises)], HANDELSBLATT AUTO GIPFEL 2022, (Nov. 8, 2018),

[9]

Toshiba Memory Europe will provide its high-density solid-state drives to OSR's EVOLVER "Datacenter on Wheels" Platform

February 22, 2019

Toshiba Memory Europe GmbH and OSR Enterprises AG (OSR), creator of the EVOLVER automotive platform for connected, autonomous, shared and electric mobility, announce today that they will extend their collaboration on OSR's in-car Datacenter to enhance live data management and logging in cars. The cooperation will combine the technical know-how of both companies and will create a "Datacenter on Wheels" with high-density and low-power solid state drives.

OSR's EVOLVER is a high-performance central "AI brain" for ultra-smart, autonomous and securely networked vehicles. The hardware and software platform reinvent the in-vehicle architecture, provides the computing power for the car of the future and operates as a central data hub which stores, processes and analyzes real-time data for artificial intelligence and analytical insights. The data and information are crucial for autonomous driving, customized user-experiences and is the foundation for new automotive business models.

[10]

OSR has continued to use this phrase as a central theme in its marketing through the present.

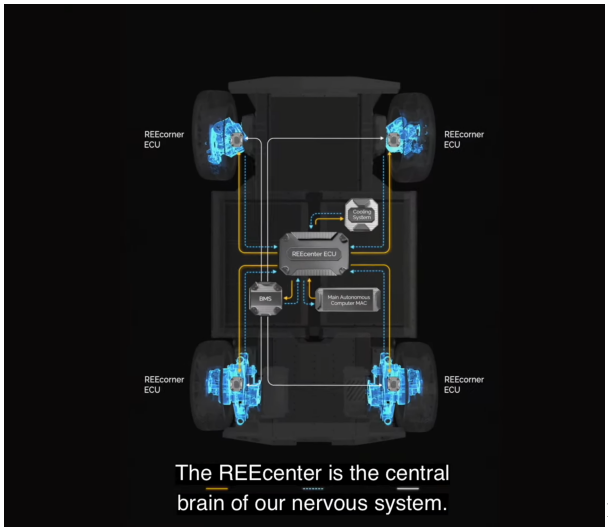
---

https://veranstaltungen.handelsblatt.com/autogipfel/interview-orit-shifman/ (translated from German).

[9] OSR 2017 IAA trade show presentation.

[10] *See Toshiba Memory Europe and OSR Enterprises AG Extend Their Collaboration to Provide In-Car Datacenter Services*, AUTOMOTIVE WORLD, (Feb. 22, 2019), https://www.automotiveworld.com/news-releases/toshiba-memory-europe-and-osr-enterprises-ag-extend-their-collaboration-to-provide-in-car-datacenter-services/.

164. REE too adopted this language in referring to the REEcenter as a "central brain," as shown in still images taken from a May 2021 REE marketing video, below:

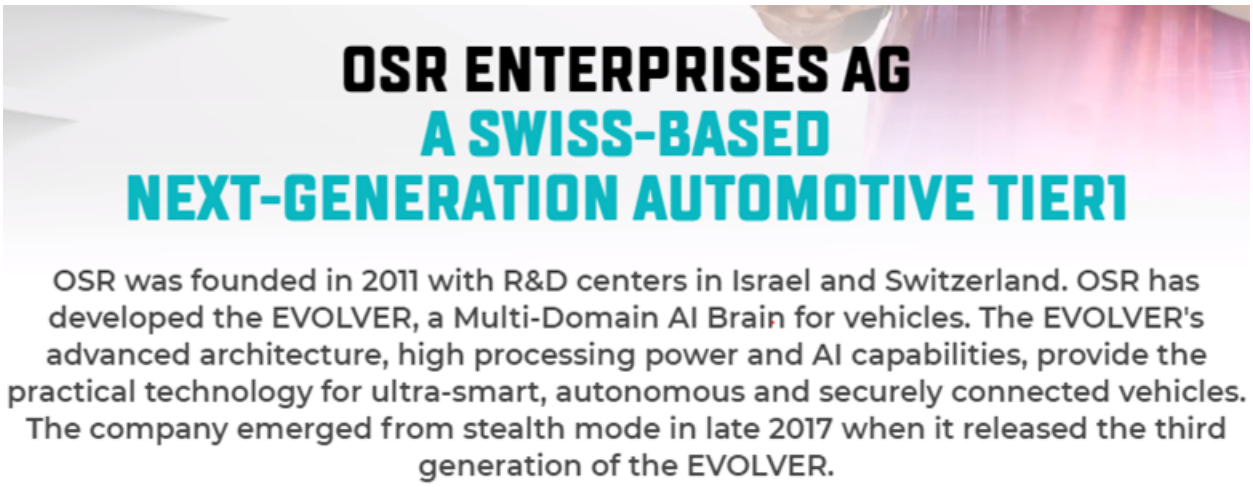


[11]

(*See also infra* at ¶¶ 176, 178, 222.)

165. Further, OSR has consistently referred to the EVOLVER's capabilities that extend past autonomous driving into, among other things, insurance uses, preventative maintenance, route optimization, and fleet management since 2017 as a "multi-domain AI Brain":

[11] *See Ohad Stauber, VP R&D, REE Automotive*, *supra* at n.6.



REE refers to its REE Platform's pilfered similar abilities as "multi-dimensional":

V. THE STOLEN TRADE SECRETS

166. A comparison of REE's sudden developments with the trade secrets in the EVOLVER, in light of the proprietary Stolen Files and contractually-restricted know-how of OSR's Former Employees that REE stole, provides damning evidence of REE's willful misappropriation. As described further below, OSR's trade secrets relate to, among others: (1) artificial intelligence and data processing to enable enhanced vehicle functions and predictions; (2) data collection and processing; (3) data storage and transfer; (4) using artificial intelligence

and data processing to enable enhanced vehicle functions and predictions; (5) universal adaptability—i.e., creating a control system capable of working in a wide variety of environments; (6) command functions, i.e., providing instructions to the vehicle's various systems; (7) cybersecurity; (8) functional safety and regulatory approval; (9) unique software tools for car OEMs; (10) customer, component, and configuration data; (11) hardware and software architecture for a multi-domain "central brain," and (12) other information.

167. Because the software and hardware did not previously exist, or did not exist in a form that could be used with the EVOLVER, OSR could not purchase them ready-made from vendors. Instead, OSR spent years painstakingly, among other things, developing and editing custom source codes for its software, unique cloud applications, designing hardware to incorporate the software and fit to function inside of a car, and extensively testing the software and hardware. Creating and arranging this information was an iterative process that required experimentation, research, and expertise at great expense, all of which are incorporated into the trade secrets and make them derive independent economic value from the fact that they are not known outside of OSR. Indeed, the entire concept of a single brain for a vehicle is OSR's invention.

168. Additionally, during the EVOLVER's development process, OSR, and OSR's employees, gained significant "negative" know-how, i.e., knowledge of design flaws and weaknesses learned during the development process that competitors can use to avoid pursuing dead ends, thereby saving them significant time and money during their own development process.

169. Among the OSR files that Stauber stole, described further below, were comprehensive sets of the EVOLVER's trade secrets, including the folder the source code and software from one of OSR's EVOLVER platforms prepared for the 2019 IAA presentations, as

well as custom software packages of the EVOLVER that OSR developed for certain of its customers.

170. Each of the trade secrets described herein derive their value from being not generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

A. Artificial Intelligence, Data-as-a-Service Functions, and Data Analytics

171. REE stole OSR's trade secrets related to artificial intelligence and data analytics. OSR developed deep learning, neural network, machine learning AI processes, and the underlying source code and algorithms, through which EVOLVER processes, analyzes, and learns from data collected throughout the vehicle and makes decisions for numerous functions including automated driving cabin monitoring, as well as the numerous multi-domain and Data-as-a-Service functions, including route optimization, insurance, preventative maintenance, and fleet management. (*See supra* at Part I.B.)

172. Because the analysis of data sets varies depending on its use, OSR accordingly developed different source codes for specific analytical methods for various uses. For example, OSR has developed specific source code that analyzes data most relevant to automobile insurance companies, such as a driver's acceleration and braking habits, among others. The EVOLVER can also provide valuable fleet management services. For example, if a fleet of vehicles is equipped with the EVOLVER, the EVOLVER's data analysis capabilities enable it to identify potential problems in a single vehicle fleet, such as a cybersecurity attack, and transmit the necessary information to all other vehicles in the fleet to protect against similar attacks on other vehicles.

173. The inherent nature of well-developed AI is that it learns and improves over time through experiences it encounters. OSR's proprietary AI took years to develop not only because

of the time engineers had to take to write and edit the code but because of the code evolved over time based on years of data the AI accumulated and adapted to through laboratory and field testing, certain of which is known to the Former Employees.

174. OSR's trade secrets concerning these AI processes consist of source code, unique methods and algorithms, embedded software solutions, and research and laboratory test results, including concerning efficient methods and inputs to train an AI as well as the various commercial requirements and methods to perform different multi-domain and data-as-a-service functions. They also consisted of failed methods, sources, algorithms, and inputs for each of the foregoing.

175. The Stolen Files known to OSR to contain these trade secrets include, among others, the IAA2019\software\EVOLVER\apps folder. Some of the trade secrets were also known to all of the contractually restricted Former Employees, but in particular Ohad Stauber, Ron Lupovici, Alex Liberman, Yossi Varman, Alex Triochin, and Eli Sidi.

176. That REE is improperly using these trade secrets is clear from the REE Platform's sudden transformation to an AI-powered "central brain" that is "responsible for . . . high-level decision making and vehicle dynamics decisions" with "multi-dimensional data as a service capabilities with our proprietary AI driven software" including "preventive maintenance," "fleet management, route optimization, insurance, and maintenance as a service."[12]

177. REE suddenly began touting in investor presentations as a key competitive advantage its purported "Autonomous Drive" capabilities, described as "REE technology designed to manage all vehicle dynamics functions, allowing for smoother and safer autonomous driving and faster time to market," its "Preventative Maintenance AI," and how "[a]doption of REE

[12] *See Ohad Stauber, VP R&D, REE Automotive*, *supra* at n.6.

technology can facilitate [Advanced driver-assistance systems] Technology implementation through to Level 5," which refers to autonomous driving.

178. Additionally, in its August 2021 report, Cowen referenced the REEcenter as the "primary 'brain'" of the platform that controls "all corner level functions." It also noted REE's intention to launch vehicles for "autonomous delivery" and highlighted REE's predictive analytics, based on its integration of neural net AI technology and preventive maintenance capabilities. Cowen also predicted that REE may have additional future opportunities through its "predictive and prescriptive neural net AI technology used to not only monitor the health and performance of a vehicle but also [to] draw operational conclusions" for fleet optimization. These are exactly some of the capabilities of the EVOLVER platform that REE stole. Cowen also reiterated that REE's technology can facilitate advanced driver-assistance systems up to level 5 autonomous driving.

179. And at the end of 2021, REE announced its "Leopard" vehicle, which it describes as an "autonomous last-mile delivery concept vehicle." This is functionality made possible by OSR's trade secrets, not by REE's own development of autonomous technology.

B. Data Collection and Processing

180. REE stole certain of OSR's trade secrets concerning OSR's unique methods of data collection and processing. Specifically, the EVOLVER collects and processes data at ultra-high rates—from all of a vehicle's various sensors, including cameras, microphones, ECUs, positional devices, and other car components—which is necessary for autonomous driving, mechanical calibration, and multi-domain or data-as-a-service functionalities. It also collects data for events—for example how the car or driver reacts while driving at a particular speed and another car moves

in front of it at a certain distance—so that other functions of the EVOLVER can learn from and adapt to that data, as well as similar data collected by other cars equipped with the EVOLVER.

181. The EVOLVER's data collection and processing functionality is unique in that it can be connected to many data sources simultaneously and process the data from those sources simultaneously. The EVOLVER also supports sensors of many types from different manufacturers. These capabilities required significant development time and resources and involved long specification and development processes including with OSR's OEM customers to ensure compatibility with different OEM's sensors and vehicle setup.

182. OSR's trade secrets concerning this data collection and processing consists of, among other things, source code and unique methods as well as research results, unique hardware designs, schematics, specifications, and methods of connection, related to connecting to the car's components where the data originates, sensor initialization and configuration, and collecting and processing the data. They also include failed methods and designs for the foregoing.

183. Stauber illegally copied to external drives technical information regarding data collection software source code and hardware designs that constitute OSR trade secrets. Stauber's theft also included design schematics that are essentially blueprints for the main circuit board in the EVOLVER showing its configuration and connections, which OSR took years to develop and determine (the "Stolen Schematics"). The Stolen Schematics are comprehensive and would permit a competitor to copy OSR's design for immediate use.

184. Stauber also stole data sheets from OSR containing its trade secrets, which identify, among other things, laboriously sourced, researched, and tested hardware components and suppliers which OSR had discovered, after lengthy research, provided the most efficient solutions for OSR's requirements. These data sheets also include design specifications for connecting the

hardware in optimal ways, and specific hardware processes, such as, for example, initialization sequences ("Stolen Data Sheets").

185. The Stolen Files OSR was able to discover containing these trade secrets, include, among others, the IAA2019 folder, the TAMIR folder, the Gulliver folder, release_experimental…..zip, AP12_DS_Oct_2016, and POS LV Datasheet.[13]

186. In violation of OSR's policies, Stauber also took pictures using his personal cellphone of proprietary hardware designed by OSR, including circuit boards and connectors, as well as the confidential names of OSR's suppliers (the "Stolen Photographs"). OSR's investigation determined that Stauber sought to cover his tracks by deleting copies of emails containing these pictures from the Stauber Laptop and Stauber failed to surrender them when he left.

187. Further, given that data processing and collection is one of the core capabilities of the EVOLVER, each of the contractually-restricted Former Employees worked on, and had knowledge of, these trade secrets, and in particular, Stauber, Lupovici, Liberman, Sidi, Teryohin, and Rodman.

188. That REE is improperly using these trade secrets is evidenced by, *inter alia*, comments made by Stauber himself in early 2021 shortly after REE started discussing the REEcenter in marketing materials as an "autonomous ready," centralized AI platform: "'REEboard and REEcorners are 'smart.' They're designed to accommodate sensors for deep and robust data gathering, allowing for storage, analytics." REE's "data harvesting" abilities,

[13] Even disclosing specific names of many of these files could reveal OSR's trade secrets inasmuch as they reflect, to those skilled in the art, certain proprietary methods as well as confidential components, clients, or partners.

including "logging all sensor data for offline and cloud-based analysis," were also touted in Cowen's August 2021 report.

C. Data Storage and Transfer

189. REE stole OSR's trade secrets concerning OSR's unique methods of data storage and transfer. Many of EVOLVER's functions, such as the data collection described above (*see supra* at ¶¶ 59, 62, 180-82) require significant data storage and transfer capabilities. Thus, to implement this functionality, OSR had to develop and perfect hardware and software techniques and solutions for high-bandwidth and high-capacity physical data storage in a centralized computer platform that are able to store and provide adequate data transfer rates for the large amounts of data collected from all of the car's systems, sensors, and other components, and to efficiently manage the long- and short-term (called "RAM") data memory. Additionally, OSR had to develop source code for storing, timestamping (also with specificity to the millisecond), and processing the collected data (*see supra* at ¶ 180) within the physical data storage system in a way that enables the EVOLVER platform to access it in order to perform data analytics (*see supra* at ¶ 172).

190. OSR's EVOLVER platform's ability to store this amount of data and utilize it with ultra-short latency (i.e., minimal delay) in a synchronized manner is unique and crucial in the autonomous vehicle industry because of the need for self-driving cars to make decisions and actuate nearly instantaneously to protect the safety of the passengers and the car's surrounding environment, among other reasons. Developing the EVOLVER's data storage and transfer capabilities was time consuming and expensive, including lengthy "trial and error" development processes within OSR and for its OEM customers. Further, as with many other applications in the EVOLVER, there were no "off-the-shelf" tools to do this.

191. OSR's trade secrets concerning this data storage and transfer consists of, among other things, dedicated software and source code, unique methods, research results, and unique hardware designs, schematics, and specifications. They also include failed methods and designs for the foregoing.

192. These trade secrets were embodied in, among other things, source code, Stolen Schematics, Stolen Data Sheets, and Stolen Photographs. The Stolen Files OSR was able to discover containing these trade secrets, include, among others, the IAA2019\software\EVOLVER\apps folder, in a 256b folder (including files with the extensions STP, JIC, HEX, MAP, TXT SOPCINFO), and in the Stolen Photographs.

193. Further, given that data processing and collection is one of the core capabilities of the EVOLVER, each of the contractually-restricted Former Employees worked on, and had knowledge of, these stolen trade secrets.

194. REE's misappropriation is again evidenced by Stauber's 2021 comments concerning its centralized AI platform designed to accommodate sensors for "Deep and robust data gathering, allowing for storage, analytics."

D. Universal Adaptability

195. REE also stole OSR's trade secrets developed to make the EVOLVER installable in, and adaptable to, a variety of non-autonomous vehicles. Building out this system required extensive and laborious research and testing concerning the configurations and performance in different vehicles with different components and ECUs, as well as hardware and software methods to control those varying functions and processes.

196. OSR's trade secrets are embodied in the source code, software and hardware architecture, design, and configuration of the EVOLVER itself, which is highly adaptable,

including the Stolen Data Sheets, Stolen Photographs, and Stolen Schematics and in each of the Stolen Files listed herein, among others. They also consist of methods, research and test results, including failed methods, known to each of the contractually-restricted Former Employees. In particular, in addition to Stauber, the Former Employees all had access to these trade secrets, depending on their particular disciplines, including hardware, software, embedded software, and mechanics.

197. That REE is improperly using these trade secrets is evidenced by the fact that its purported core competency is configurability to a variety of different applications. For example, Barel has advertised the REE Platform as "the perfect blank canvas for our customers on which to build EVs tailored to their needs, whether it's a fully autonomous last-mile delivery vehicle, a spacious yet compact urban shuttle or a flexible delivery truck with higher load capability on a smaller footprint," for vehicles with "any shape, any size, any weight, any kind of body technology and autonomy."

198. Moreover, REE has advertised its platform as "autonomous ready." To suddenly make a previously mechanical EV platform "autonomous ready" required the use of OSR's proprietary trade secrets that can permit regular cars to become "autonomous ready."

E. Command Functions and Actuation, Including "Drive By Wire"

199. REE stole OSR's trade secrets related to command functions and actuation. OSR also had to develop software and design hardware components to connect the decisions made by the AI to the actuation of vehicle systems, such as steering and brakes by means of remote electronic control, as opposed to traditional mechanical and hydraulic control systems, known as "drive-by-wire" or "X-by-wire." In an "X-by-wire" system, a driver's input, such as turning a steering wheel, generates an electronic signal that prompts an ECU to actuate an electric motor,

which then adjusts the steering angle accordingly, without any direct mechanical linkages between the steering wheel and the wheels themselves. OSR has developed command functions and actuation not only to convert a regular vehicle to autonomous, but also to operate remotely. The EVOLVER has taken drive-by-wire to new limits, capable of controlling vehicles completely remotely, including via a remote VR headset.

200. OSR's trade secrets also included applying the AI decision making to actuation for regular, self-driving cars using robotics. These trade secrets were embodied in the source code and hardware architecture and configuration of the EVOLVER itself, which is highly adaptable, including the Stolen Data Sheets, Stolen Photographs, and Stolen Schematics and in each of the Stolen Files listed herein, among others. They also consist of the methods, research and test results, including failed methods, that were known to the Former Employees together or in part. In particular, in addition to Stauber, Former Employees Eli Sidi, Alex Liberman, Denis Rodman, and Ron Lupovici worked on and were aware of these trade secrets in the course of their employment at OSR.

201. That REE is improperly using OSR's trade secrets concerning command actuation is evidenced by REE's statement that the REEcenter is "responsible for all [of the REE Platform's] high-level decision making and vehicle dynamics decisions. For example, upon making a turn at high speed, the REEcenter will decide what is the exact steering angle of each wheel, what is the exact torque and breaking power of each wheel, and whether we should activate torque vectoring capabilities." REE's X-by-wire functionality was touted by REE's investment adviser Cowen as a key feature of REE's technology, stating that REE would be the first to market with X-by-wire technology that is "agnostic" to the vehicle's power source. Indeed, Cowen described X-by-wire as "a critical part of the REEplatform design [that] yields many engineering and safety

advantages." REE's X-by-wire technology can be applied to autonomous driving and includes "proprietary full steer-by-wire, break-by-wire [*sic*] and drive-by-wire" with "no mechanical linkages between the handwheel to the pedal box too the actors on the REEcorners, or between the REEcorners themselves."

202. While REE demonstrated at the IAA 2019 show its basic remote-control driving of a dummy model—based on technology that is widely and inexpensively available in remote-controlled toy cars—it was clear that REE required substantial development. REE found a shortcut to that development in OSR's trade secrets.

F. Cybersecurity

203. REE stole OSR's trade secrets related to cybersecurity. It is critically important for autonomous cars to be protected from cybersecurity threats for safety reasons—by way of example, OSR's programmers demonstrated the vulnerability of conventional vehicles to cybersecurity threats by hacking a car and forcing it to brake, an attack that could easily result in a traffic collision. To ensure that EVOLVER was protected from cyber threats and compliant with various international regulations, OSR engaged in significant research and analysis relating to cybersecurity vulnerabilities for autonomous and artificial intelligence vehicles, and developed proprietary hardware and software solutions, to implement cybersecurity defenses in the EVOLVER and for the entire car.

204. The EVOLVER's unique cybersecurity solutions relate to the entire vehicle and are capable of monitoring the car's various systems and components for anomalies and protect the vehicle both internally (with respect to communications between different domains and buses within the vehicle) and externally (with respect to threats from connections to the internet or external devices). Further, if the system detects an anomaly, the cybersecurity solutions enable

the EVOLVER to isolate the system affected by the attack to keep the vehicle safe, preventing safety threats from ever materializing. OSR's cybersecurity research and solutions required hundreds of thousands of hours of research by top experts in Israel on behalf of OSR, including the former head of the Israeli Defense Forces cybersecurity unit. This research and development spanned years and required OSR to constantly update and build upon past research in light of emerging threats, and the results of this research (regarding both successful and unsuccessful cybersecurity approaches) and implementation of proprietary cybersecurity mechanisms comprise trade secrets that are critical to the cybersecurity of EVOLVER. These trade secrets place the EVOLVER years ahead of any products offered by OSR's competitors with respect to their cybersecurity protections.

205. OSR's trade secrets were embodied in the source code and hardware architecture and configuration of the EVOLVER itself, including the Stolen Data Sheets, Stolen Photographs, and Stolen Schematics and in the Stolen Files listed herein, among others, including in the Evolver 300 folder and cyber portfolio files. They also consist of the methods, research and test results, including failed methods, that were known to the contractually-restricted Former Employees and in particular Ohad Stauber and Ron Lupovici.

206. That REE is improperly using OSR's trade secrets is evidenced by its statements that, with the development of the REEcenter, REE had suddenly developed the ability to block malware attacks (i.e., cybersecurity threats) "via proprietary protocols." Further, cybersecurity is a practical and regulatory prerequisite to creating an advanced, computerized vehicular control system. Additionally, REE's cybersecurity technology was promoted in the August 2021 Cowen report, which specified that REE's analytics are "protected from malware attacks via proprietary protocols" and that all data collected use a "separate protected CAN."

G. Functional Safety and Regulatory Compliance

207. REE stole OSR's trade secrets related to functional safety and regulatory compliance. Since 2011, OSR engaged in extensive research and analysis relating to the functional safety of the EVOLVER platform including conducting case studies to determine international regulatory compliance. In order to ensure that the EVOLVER complied with the high levels of safety required in the automotive industry, OSR engaged in significant research to determine how best to maximize the safety of the vehicle, the driver, and passengers, including developing case studies. These case studies provide OSR, or its competitors, with the necessary information to develop safe vehicle systems and to avoid unsafe designs, including the techniques to analyze these systems to determine whether they meet safety parameters.

208. The Stolen Files OSR was able to discover containing these trade secrets, include, among others, P1H-C_Safety_Case_OSR_190722.zip. These trade secrets and the results of OSR's research were also known, in part, to the Former Employees and, in particular, Ohad Stauber and Ron Lupovici.

209. That REE is improperly using OSR's trade secrets is evidenced not only by the fact that meeting safety requirements is a necessity to going to market, but by the fact that REE advertises that its product is ISO 26262 and ASIL D Pre-Certified, which certifications were likely obtained using OSR trade secrets, given the difficulty and length of time in meeting such certification requirements. Indeed, REE has a dedicated homologation engineer based in the United States who, upon information and belief, used OSR's trade secrets in the regulatory approval process.

H. Thermal Management

210. In order to perform the above-described AI, data, and command functions without overheating, OSR also needed to develop proprietary hardware and software methods of thermal

management, which were also worked on by Ohad Stauber, Ron Lupovic, Alex Liberman, Denis Rodman, and Dmitri Gurevich. These trade secrets relate, among other things, to the placement, arrangement, combinations, and identity of the various components, the methods of efficiently running the electronic and components, as well as methods for building an enclosure capable off efficiently housing the components without overheating. They also include failed methods and designs for the foregoing.

211. To obtain these trade secrets, REE recruited Dmitri Gurevich as its thermal hardware engineer. Gurevich led a mechanical department in OSR and was responsible for continuing to develop OSR's mechanical enclosure and thermal management system. REE also advertised that its suddenly developed REEcenter contains a thermal management system.

I. Unique Software Tools for OEM Customers

212. OSR has also developed over many years a unique set of tools allowing OEM customers to customize the configuration of the EVOLVER to their specific vehicle setups, such as the use of sensors from certain manufacturers or for collecting certain data, and to select à la carte functions of the EVOLVER.

213. This set of tools was developed within OSR in order to support OSR's automotive OEM customers, taking into account OEM customers' desired specifications and unique needs and working with manufacturers of sensors and ECUs. These tools enable OEM teams around the world to work together in one environment and to substantially shorten the time necessary to bring an autonomous or semi-autonomous vehicle to market. In addition, it enables OSR or the OEMs using the technology to create tailor-made designs and configurations for each vehicle model and to run simulations for various environments and weather conditions. These tools were provided to specific chosen teams within OEM customers of OSR, under strict confidentiality agreements.

OSR's trade secrets also include internal lists of its OEM customers and what OSR learned about preferences for specific configurations of the EVOLVER.

214. The trade secrets consist of OSR's source code, methods of customization and collection, and internal research concerning customers as well as what OSR determined to be those customers' preferences. OSR's trade secrets also consist of the knowledge of OSR's Former Employees Ohad Stauber, Alex Liberman, Yossi Varman, Denis Rodman, and Eli Sidi concerning this code, methods, and research.

215. The Stolen Files OSR was able to discover containing these trade secrets, include, among others, a folder Stauber had copied to the Stauber Laptop and deleted, called "TAMIR," to which Stauber should not even have had access.

216. That REE is improperly using OSR's trade secrets related to OEM tools is evidenced by the fact that its claimed core competency is configurability to a variety of different applications and its advertisement as a key competitive advantage of multi-dimensional services, which necessarily, must be configurable to meet a customer's individual needs. For example, Barel has advertised the REE Platform as "the perfect blank canvas for our customers on which to build EVs tailored to their needs, whether it's a fully autonomous last-mile delivery vehicle, a spacious yet compact urban shuttle or a flexible delivery truck with higher load capability on a smaller footprint."

J. Customer, Supplier, and Component Information

217. Through the course of its decade in building the EVOLVER and working with customers, OSR developed extensive knowledge concerning the best components and suppliers with whom it worked for the applications described herein. OSR also learned about the preferences

of its customers and potential customers. OSR's closely-guarded knowledge is incredibly valuable and cuts significant time in research and development as well as marketing.

218. Each of the Former Employees knew of certain of those trade secrets.

219. That REE is improperly using these trade secrets is also evidenced by its impossibly short "development" time following the hiring of the Former Employees who had direct knowledge of these developments. REE has also tried to develop relationships with several of OSR's partners, which, upon information and belief, it did with the benefit of OSR's trade secrets.

K. Hardware and Software Architecture for a Multi-Domain "Central Brain"

220. As discussed herein, OSR's concept of using a single "central brain" to control smart and self-driving vehicles with the functions and capabilities described herein was unprecedented. To be able to control the car, including the many ECUs, through a single hardware and software solution required extensive and laborious research and testing concerning the configurations and performance in different vehicles with different components and ECUs, as well as hardware and software methods to control those varying functions and processes from a single, central repository.

221. OSR's trade secrets were embodied in the source code and hardware architecture and configuration of the EVOLVER itself, including the Stolen Data Sheets, Stolen Photographs, and Stolen Schematics and in the Stolen Files listed herein, among others, including in the Evolver 300 folder and cyber portfolio files. They also consist of the methods, research and test results, including failed methods, that were known to each of the contractually-restricted Former Employees and in particular Ohad Stauber and Ron Lupovici.

222. That REE is improperly using these trade secrets is evidenced by the fact that REE has similarly advertised the "REEcenter" as a "central brain" that is "responsible for all [of the

REE Platform's] high-level decision making and vehicle dynamics decisions" and contains X-by-wire functionality that is capable of controlling the many functions of an EV.[14]

L. Additional Trade Secrets

223. The Stolen Files also included information regarding the proprietary software and hardware developed by OSR relating to various other functions of the EVOLVER, including: (i) design and implications of displays for passengers, such as instrument clusters, displaying various information generated by the EVOLVER; and (ii) an electronic voice assistant—similar to "Siri" for Apple products or "Alexa" for Amazon products—that connects to the EVOLVER and functions with or without internet connectivity, can understand more terms than similar features in today's cars, and can detect emotions in the user's voice which can be used as part of the other cabin monitoring features discussed above for the EVOLVER to make decisions based on a driver's condition.

224. Although REE has not specifically announced these capabilities yet, upon information and belief it has the potential to use or develop products based on them. For example, in order to interact with the REEcenter or understand its functions necessarily requires a display function. OSR worked to develop these display functions in a manner that was both efficient and attractive. Further, to share data related to data-as-a-service with a user also requires proprietary displays.

225. These trade secrets consist of proprietary source code as well as market research and design elements not shared with the public and were contained in the Stolen Files in a folder that was confidential. OSR's trade secrets also consist of the knowledge of OSR's Former

[14] *See Ohad Stauber, VP R&D, REE Automotive*, *supra* at n.6.

Employees Ohad Stauber, Alex Liberman, Yossi Varman, and Eli Sidi concerning OSR's market research and design knowledge.

M. Non-Trade Secret Confidential Information

226. Additionally, any information taken by or later obtained by any Defendant, even if not specifically a trade secret, is nevertheless highly confidential and owned by OSR. OSR has not authorized any Defendant to access or possess any of its confidential information, regardless of whether such information falls within the definitions of trade secrets.

VI. REE'S USE OF OSR'S TRADE SECRETS IN THE UNITED STATES

227. Despite OSR's formal warnings, REE immediately put OSR's trade secrets to work in the United States to market and sell its products incorporating OSR's trade secrets to U.S. customers, to obtain visible and lucrative partnerships with U.S. companies to produce products containing them, and to secure hundreds of millions of dollars in investments.

A. REE Sells, Markets, and is Threatening to Produce Products Incorporating, Trade Secrets It Stole from OSR in the United States

228. The U.S. market is critical for REE's misappropriation, and threatened future misappropriation, of OSR's trade secrets. The majority of REE's budget is targeted towards the commercialization of REE's P7 EV platform—incorporating the stolen OSR trade secrets—in the United States and Europe. REE has stated that its "first deployment will be in the more easy, friendly states within the U.S.," from a regulatory standpoint, including in Texas. (*See supra* at ¶ 49.) REE has also represented that it expected "full vehicle customer validation on private roads in the U.S. in mid-2022."

229. In or around the Fall of 2022, REE held demonstration events for the REE Platform, including the misappropriated trade secrets, in the U.S., and had numerous companies "evaluate[] and test[]" the REE Platform in the U.S., and took orders for the REE Platform from U.S.

customers.[15] As set forth above (*see supra* at ¶ 148), REE also has taken orders for Proxima Powered by REE from, according to REE, "several leading US fleets." REE has presented and marketed its products, which prominently incorporate technology based on trade secrets it sole from OSR, at the Consumer Electronics Show ("CES") in Las Vegas, Nevada, and plans to do so again this year. REE regularly conducts interviews promoting products, which prominently incorporate technology based on trade secrets it stole from OSR, with U.S. outlets and geared for U.S. audiences, including to promote, market, and fundraise for the stolen technology

230. REE also intends to produce the REE Platform including the stolen OSR trade secrets, in the United States at its Pflugerville North American headquarters and "integration center," using proceeds from the Merger, obtained by using the stolen OSR trade secrets.

231. REE has been expanding its focus on the United States by rapidly hiring U.S.-based employees. REE has already hired more than 20 U.S. employees, including: (1) REE's Head of Product Marketing, who has made statements regarding the REEcenter and the stolen OSR trade secrets in filings made with the SEC; (2) a quality assurance manager based in Texas who specializes in "plant start-ups"; (3) a homologation engineering director in California who, upon information and belief, has relied upon the stolen OSR trade secrets; (4) a recruitment specialist focused on the US; (5) a supplier quality manager; and (6) a number of attorneys focused on intellectual property who threaten to place OSR's technology at risk by filing patent applications

[15] *See REE Automotive Ltd. (REE) Q3 2022 Earnings Call Transcript*, SEEKING ALPHA (Nov. 16, 2022), https://seekingalpha.com/article/4558521-ree-automotive-ltd-ree-q3-2022-earnings-call-transcript; *Morgan Olson, EAVX and REE Automotive host customer evaluations for Proxima Powered by REE, a newly-designed electric walk-in step van*, REE (July 25, 2022), https://ree.auto/press-release/morgan-olson-eavx-and-ree-automotive-host-customer-evaluations-for-proxima-powered-by-ree-a-newly-designed-electric-walk-in-step-van/.

that disclose OSR's technology. Many of REE's US employees are based in Texas, as discussed above.

232. REE also submitted its website to the United States Patent and Trademark Office in connection with its representation that it is using the mark REE in "interstate commerce," as defined in 15 U.S.C. § 1127. This requires that REE use its mark to actually sell its products and/or services in the United States. Further, REE represented that it was using its mark for products and services, including with respect to "motor vehicle inspections and roadworthiness testing," which is based on and copies OSR's predictive maintenance technology, which REE stole.

B. REE Discloses OSR's Trade Secrets through Partnerships with U.S. Companies

233. REE is also entering into partnerships with companies through which it is likely to, or already has, disclosed the stolen OSR trade secrets and which will allow REE and/or its partners to sell products containing the stolen OSR trade secrets.

234. As described above (*see supra* at ¶¶ 35, 46, 148), REE entered into a partnership with Texas-based EAVX to develop the Proxima Powered by REE vehicle, based on REE's P7 platform. REE also announced that it will be providing test vehicles to "some of the world's largest rental fleet and commercial truck retailers in North America." Thus, the stolen OSR trade secrets have been disclosed to EAVX, and through REE's partnership with EAVX, to countless other fleets and retailers.

235. REE also has agreements to provide its own P7-B electric box truck to "multiple large fleet operators in the United States," with one fleet operator introducing the P7-B to its US-based fleet for use by Fortune 500 company customers. As these vehicles become commercially available and are provided to additional third parties, REE will disclose the trade secrets it stole from OSR, which serve as the basis for REE's products.

236. REE has also partnered with American Axle & Manufacturing ("AAM"), an American company headquartered in Detroit, Michigan. AAM is a manufacturer and designer of drivelines (i.e., the mechanical components that transfer power from the engine and transmission of a car to the wheels). Upon information and belief, these components will be controlled with technology based on trade secrets that REE stole from OSR and those stolen trade secrets were or will be disclosed in order to incorporate the drivelines into the REE platform.

237. REE has also partnered with Kansas-based Koch Industries, Inc., whose subsidiary Koch Strategic Platforms, LLC, a Delaware limited liability company, is a substantial REE investor.

238. These partnerships, and others, will result in the disclosure of the stolen OSR trade secrets in order for the REEcenter to be incorporated into and connected to the vehicles and components manufactured in partnership with EAVX, AAM, and others. Indeed, REE announced that the orders followed "extensive due diligence by our customers."

239. With the announcement of REE's integration center and U.S. headquarters, along with its partnerships with U.S. companies, confirmed product orders, and other facts described herein, REE's intent to proceed with using trade secrets stolen from OSR, and acts in furtherance in the U.S., have become crystal clear.

C. REE Uses OSR's Trade Secrets to Go Public

240. REE used OSR's trade secrets to drive interest in its company to go public through a SPAC transaction in 2020 and 2021. In December 2020—shortly after Stauber joined REE—REE and a SPAC called 10X began discussions concerning a potential merger that would allow REE to bypass the laborious initial public offering process to become a public company listed on

the NASDAQ. REE told 10X that it needed to raise up to $500 million in total in order to execute its strategy and bring a product, based on OSR trade secrets, to market.

241. 10X was not interested in merging with a company that was aiming to develop a mere mechanical platform, much less one that had no real differentiation from competitors. Rather, 10X had "focus[ed] [its] efforts on identifying high-growth technology and tech-enabled businesses [in] . . . industries that are being industries that are being disrupted by advances in technology and on technology paradigms including artificial intelligence ("AI"), automation, data science, ecommerce and Software-as-a-Service ("SaaS")." REE was concerned that the "REEcorner" and "REEboard" concepts were too similar to pre-existing competitors, which were further along in the development process, for REE to have any substantial independent value (*see supra* at Part III.B), and 10X's mandate regarding AI and automation could not be further away from REE's original mechanical platform. But with the inclusion of the version of the AI brain platform REE stole from OSR, including OSR's strong data science and data-as-a-service offerings, the REE Platform fell squarely within 10X's mandate. Accordingly, REE needed to rely completely on OSR's trade secrets it had managed to obtain to differentiate itself to 10X.

242. OSR's trade secrets were critical to 10X's assessment of value. In a preliminary proxy statement filed with the SEC, REE in particular highlighted as "competitive strengths," REEcenter's preventative maintenance functionality, claiming that the REE Platform's "predictive maintenance scheduling through smart service and maintenance AI" and "data harvesting capabilities [which] may be used to further reduce [total cost of ownership] via intelligent preventative maintenance features"—all functionality that was mirrored by stealing OSR's trade secrets.

243. REE therefore used OSR's trade secrets to secure 10X's investment and "go public." Further, prior to entering into a definitive merger agreement, 10X conducted substantial due diligence during which time, upon information and belief, REE disclosed the trade secrets it stole from OSR.

244. 10X ultimately decided to enter into the merger agreement because it concluded that REE offered "clear competitive advantages over competing electric vehicle drivetrain, platform and by-wire solutions, including conventional 'skateboards' and in-wheel/hub motor technology." In other words, 10X acknowledged that competitors also had "skateboards" and "in-wheel/hub motor technology," like REE's REEboard and REEcorners, but believed that REE was differentiated by advantages completely derived from OSR's stolen trade secrets.

245. On February 3, 2021, REE and 10X jointly announced in a press release issued from New York and Tel Aviv that the two had entered into a merger agreement for a business combination that would result in REE becoming a publicly listed company on the NASDAQ stock exchange, based in New York. The Merger closed on July 22, 2021.

246. In the Merger agreement, REE represented that it was not aware of any threatened legal proceedings against it or any "facts or circumstances that would reasonably be expected to give rise to any material [l]egal [p]roceeding," despite multiple letters that OSR had sent REE relating to Stauber's theft of OSR's trade secrets, REE's employment of Stauber and attempts to lure away additional OSR employees, and the notice to REE of OSR's intent to protect and enforce its intellectual property rights.

247. REE's submissions to the SEC prior to the Merger, including the definitive proxy statement filed by 10X on July 1, 2021, falsely claimed that REE owned or had a license to REE's core intellectual property and that REE has a "track record of invention and early development of

products . . . across hardware and software," when in fact it did not. And specifically, REE claimed in the definitive proxy statement that its platform had capabilities that actually belong to OSR, including autonomous driving, artificial intelligence and data harvesting, preventative maintenance features, X-by-wire control, and cybersecurity protection, among others.

248. In its August 2022 registration statement filed with the SEC, REE falsely represented that it owns or has a valid license to all intellectual property, including trade secrets, necessary for its businesses, claiming that "the Company and its subsidiaries own or have a valid license to all patents, inventions, copyrights, know how (including trade secrets and other unpatented and/or unpatentable proprietary or confidential information, systems or procedures) . . . used or held for use in any material respect, or reasonably necessary to the conduct of their respective businesses." REE made this statement despite OSR's repeated warnings, discussed below, concerning REE's unlicensed use of OSR's technology.

249. REE entirely failed to disclose its theft, and OSR's warnings regarding the theft, to prospective partners, the public, the SEC, or most investors, instead passing off the stolen technology as its own. Apparently some select investors, however, received notice. When the Merger closed, less than two weeks after OSR sent a letter to 10X, approximately $150 million of the $500 million of initial investments, accounting for 75% of the redeemable shares, were redeemed. REE and 10X replaced this cash with funds from a few, large institutional investors, whom they kept in the dark. These redemptions represented an unusually large percentage of the initial investors, and were mostly by large institutions and professional investors, many of whom, upon information and belief, had ties with REE.

D. REE Focused Its Fundraising Efforts on the United States

250. As discussed above and herein, REE has raised a substantial portion of its funding by promising a product based on OSR's stolen trade secrets to investors in the United States. These investments have enabled REE to enter into partnerships with companies in the U.S. and abroad to produce the product.

251. Specifically, REE and 10X, including by and through their United States-based agents, have extensively marketed the REE Platform to investors and financial analysts in the United States through roadshows and other presentations. REE continued to emphasize the REEcenter, which is entirely based on the trade secrets stolen from OSR, as the main element of its technology in materials REE used for roadshows, investor presentations, and other marketing connected to the Merger, including but not limited to pitch decks, videos, filings with the Securities and Exchange Commission, and during appearances—including by Barel and Stauber—on United States financial and online media outlets.

252. For example, on the same day the Merger was announced and on the ensuing days, REE CEO Daniel Barel was interviewed about the Merger and the REE Platform by several United States-based investors and financial news platforms, including Bloomberg, Yahoo! Finance, and TD Ameritrade Network. These interviews were available for viewing in the United States by United States investors and REE filed transcripts for them with the SEC.

253. Similarly, in investor pitch decks, REE has touted numerous features of the REE Platform which were taken in whole from the EVOLVER, including "Preventative Maintenance AI," cyber security," autonomous drive, and data-as-a-service. (*See supra* at Part IV.A.) Investor presentations also included a photograph similar to the one set forth above in paragraph 145, that featured the REEcenter incorporated in the middle of the REE Platform. In registration statements filed with the SEC, REE's key argument for investment were based on competitive advantages

that in fact were supplied by the trade secrets REE stole from OSR, which REE falsely attributed to itself. (*See supra* at ¶ 242.)

254. REE's efforts were successful in raising substantial funds from investors in the U.S. Pursuant to the Merger, certain investors entered into subscription agreements for a PIPE investment of $300,000,000 in exchange for equity in 10X. Upon consummation of the Merger, 10X became a subsidiary of REE, and the PIPE investors became equity holders in REE. At least one—and, on information and belief, more—of the PIPE investors is based in the United States.

255. Further, a trust account containing over $200,000,000 from the proceeds of 10X's initial public offering and the sale of warrants was, on information and belief, transferred to REE upon consummation of the Merger. A significant portion of these funds are from United States investors, including 10X Capital SPAC Sponsor I LLC (incorporated in Delaware), and, on information and belief, several of 10X's largest investors based and headquartered in the U.S.

256. REE's U.S. agents were key to obtaining these investments, and therefore furthering their misappropriation. REE and 10X engaged a U.S. investor relations specialist to pitch investments in REE, both from the investing public and through private placements. The investor pitches were based on technology copying the trade secrets stolen from OSR. REE and 10X further engaged Morgan Stanley, a U.S. bank, to serve as a placement advisor for private placement in public equity ("PIPE") investments (investments that are purchased below the market price, often by large institutional investors).

257. REE also engaged Cowen, a New York firm, as its investment advisor. REE and 10X also engaged Frost & Sullivan, a U.S. company, to advise them on its automotive strategy and assist in due diligence. Further, in advance of the Merger, both REE Automotive and 10X retained New York counsel, White & Case LLP and Morgan Lewis & Bockius LLP, to advise

them regarding the structure of the Merger in order to ensure that REE could be publicly traded on the NASDAQ.

258. Since the Merger, REE's stock has been traded on the U.S.-based NASDAQ stock exchange. While following the Merger REE's stock was initially valued at approximately $10 per share, it quickly dropped below $10, and as of December 16, 2022, was trading as low as $0.42, a precipitous 96% drop from its peak of $10.82 in August 2021.

E. OSR Issues Formal Warnings in the United States

259. As discussed above, in or around the spring of 2021 and before the Merger was consummated, it began to appear that REE was focusing a significant portion of its fundraising (including a NASDAQ listing), marketing, and production strategy on the United States, and that this strategy was centered squarely around OSR's stolen trade secrets.

260. Accordingly, on April 24, 2021, OSR sent a letter to REE warning it that, if it continued with its misappropriation, it would be violating U.S. trade secret law if it proceeded. After REE failed to desist, and proceeded with its merger plans, OSR also sent a letter to 10X, informing 10X of its findings.

261. REE responded initially through its U.S. counsel. REE did not (and could not) attempt to rebut OSR's allegations that Stauber had stolen data or deny that they had systematically targeted OSR's employees. REE could only point to evidence that, prior to Stauber joining the company, it had been working on putting major car components in the wheel. But REE did not contest the fact that REE's purported technological leaps in centralized computing, data processing and collection, AI, and "multi-dimensional" services—all taken from OSR—only began *after* Stauber came to REE with his treasure trove of stolen files.

262. For example, REE responded to OSR only that "REE's own proprietary and innovative EV technology relating to its REEcorner and REEboard systems was well underway and developed by other REE employees long before Mr. Stauber . . . joined the company, as evidenced by the timing and content of REE's patent filings." Tellingly, REE stated only that its modular, mechanical system existed prior to Stauber joining OSR. Neither REE, nor their patent filings, contained any mention whatsoever of the "REEcenter" and all related capabilities that REE announced a year after hiring Stauber.

263. Further, while "REE is always willing to discuss and resolve disputes in good faith," it claimed that OSR's descriptions of Stauber's theft contained insufficient details—notwithstanding that all of the elements of that theft were within its own possession.

264. Subsequent to these warnings and the Merger, REE continued to promote its stolen platform, emphasizing, among other things, its X-by-wire technology, artificial intelligence, and data collection and monetization capabilities, all derived from the stolen OSR trade secrets. As alleged above, *supra* at ¶ 148, REE has continued to show the REEcenter in its promotional materials in 2022.

265. On August 5, 2022, OSR again sent REE another letter regarding REE's misappropriation of OSR's trade secrets and threatening litigation. On August 22, 2022, REE's counsel replied, refusing to negotiate a settlement, but now denying in wholly conclusory terms OSR's allegations, and referring once again to REE's unrelated patent filings.

266. On December 14, 2022, a Sergeant Major of the Israeli police confirmed to OSR that there is an investigation "currently being conducted" by a special team of the Israeli police's cybercrime division, together with the head of the division and with the guidance of an Israeli

district attorneys' office, "against Ohad Stauber and REE corporation, inter alia, under suspicion of theft and computer crimes."[16]

267. Notwithstanding OSR's demand letters, REE has continually falsely represented in SEC filings that "there is no pending or, to the Company's knowledge, threatened action, suit, proceeding or claim by others challenging . . . any rights of the Company or any of its subsidiaries in . . . [REE's] Intellectual Property Rights" and that "***neither the Company nor any of its subsidiaries has received any notice*** alleging any infringement, misappropriation or other violation of Intellectual Property Rights" (emphasis added).

VII. REE'S MISAPPROPRIATION HAS DAMAGED AND CONTINUES TO DAMAGE OSR

268. Upon its public debut, REE obtained market capitalization and valuation of $3.1 billion, which valuation was entirely based on the trade secrets stolen from OSR, given REE's failure to obtain significant outside investment or product differentiation without OSR's trade secrets.

269. The harm that REE's ongoing misappropriation of OSR's trade secrets has caused, and will continue to cause, is immeasurable. REE has been able to use the trade secrets it stole from OSR to attract investors and engineers away from competitors (competitors that now include OSR, due to REE's recent entry into the same market). This further provides REE with an unfair market position, giving REE an advantage in bringing the REE Platform to market. Early market entry has significant value, particularly in the autonomous vehicle segment, which could be worth trillions of dollars in the coming years.

[16] Translated from Hebrew.

270. Additionally, as REE continues to hire new engineers and enter into partnerships with other companies, in the United States and around the world, OSR's trade secrets will be even more at risk of unauthorized disclosure. In particular, REE intends to hire an additional approximately 150 employees at its Texas integration center, making it almost certain that REE will disclose the trade secrets it stole from OSR to countless employees in the United States.

271. And as REE approaches commercialization of the REE Platform, it is likely that OSR's trade secrets will be destroyed through REE's regulatory filings and/or patent applications, given REE's numerous hires of intellectual property attorneys in the United States. Thus, REE's misappropriation will not only harm OSR's ability to compete in their chosen market; it creates a grave risk that OSR's trade secrets will be entirely destroyed through disclosure.

272. Further, REE has stated that its manufacturing model will enable it to quickly begin and scale up manufacturing once it has completed its integration centers, meaning that REE's sale of products incorporating misappropriated trade secrets will likely increase quickly and to a significant degree, making it even more likely that the value of OSR's trade secrets will be destroyed, thereby permanently harming OSR's ability to compete.

VIII. REE AUTOMOTIVE, REE USA, AND 10X ARE ALTER EGOS OF EACH OTHER

273. REE Automotive, REE USA, and REE Holding are alter egos of each other and are all controlled by a common set of individuals who operate the businesses as a single enterprise.

274. REE Automotive stated in its Form 20-F filing with the SEC, dated March 28, 2022, that it holds 100 percent of all ordinary shares for REE USA and REE Holding. Further, in the proxy statement filed with the SEC before the Merger, REE lumps together REE Automotive with all its subsidiaries, including REE USA and REE Holding. In the proxy statement, REE stated that decisions are made at "the consolidated level" by "[REE's] chief operating decision maker":

> The Company operates in two operating and reportable segments. Operating segments are defined as components of an enterprise about which separate financial information is evaluated regularly by the chief operating decision maker, in deciding how to allocate resources and assessing performance. The ***Company's chief operating decision maker*** allocates resources and assesses performance based upon discrete financial information ***at the consolidated level***.

275. Thus, upon information and belief, REE Automotive, through its officers, exercises complete and total financial control over REE USA and REE Holding. In particular, REE USA has no independent business discretion and is operated simply as an extension of REE Automotive.

276. REE Automotive CEO Daniel Barel is the CEO and Secretary of REE USA. Further, Hai Aviv was simultaneously the CFO of REE Automotive and REE USA as of February 2022. As of March 2022, REE Automotive's current CFO, David Goldberg, had become the CFO of REE USA. The only officers or directors named in REE Holding's incorporation filings are: (1) Hans Thomas, the Chairman and CEO of REE Holding at the time of the Merger, and who is also a Director of REE Automotive; and (2) Hai Aviv, CFO and director of REE Holding, who was CFO of REE Automotive and REE USA.

277. REE Automotive, REE Holding, and REE USA, also fail to observe corporate formalities. REE USA appears to have no directors, other than Daniel Barel, and the only directors identified for REE Holding are or were insiders at REE Automotive. This shows a clear lack of corporate formalities, with REE USA and REE Holding being wholly controlled and operated by executives and directors of REE Automotive.

278. REE USA and REE Holding are underfunded and rely on financing from REE Automotive. REE has only just announced its first commercial orders, yet REE USA was able to enter into a 10-year lease for its headquarters and integration center in Texas, as well as fund construction of the integration center itself. In its SEC filings, REE has stated that the "total

estimated asset and liability value recorded on our books for this lease will be within the range of [$7,300,000] and [$9,000,000]." REE Automotive, not REE USA, was the recipient of funding as a result of the Merger; REE USA and REE Holding have no source of financing other than from their parent company, REE Automotive.

279. In sum, REE Automotive, REE USA, and REE Holding operate as a single enterprise, with minimal or absent corporate formalities, intermingled funds, and overlapping officers. REE Automotive controls REE USA and REE Holding, financing their activities to further its activities in the United States and its misappropriation of OSR's trade secrets. These three entities are alter egos of each other and should be treated as such under the law.

IX. REE USA AND REE HOLDING ARE AGENTS OF REE AUTOMOTIVE

280. REE USA and REE Holding also function as REE Automotive's agents in the United States, and specifically Texas, with respect to REE Automotive's misappropriation of OSR's trade secrets. REE USA and REE Holding act as REE Automotive's arm in the United States for researching, developing, marketing, selling, fundraising, and manufacturing products based on trade secrets stolen from OSR.

281. REE Automotive assigns the tasks of REE USA and REE Holding and controls the means and details of the process by which REE USA and REE Holding accomplishes those tasks. As described above (¶ 274), the actions of REE USA and REE Holding are the results of decisions by REE Automotive's "chief operating decision maker." REE Automotive, as the parent company, with the same executives as REE USA and REE Holding, assigns REE USA and REE Holding tasks and directs how those tasks are to be completed in Texas.

282. For example, REE Automotive directed REE USA to enter into a lease to use as the North American and U.S. corporate headquarters for REE Automotive, REE USA, and REE

Holding. REE Automotive also directed its development of a US-based "integration center" at the Texas location where REE Automotive, REE USA, and REE Holding will use OSR's trade secrets in its manufacturing of the REE Platform. Indeed, REE USA otherwise has no source of funds with which to pay rent or to build the Texas integration center.

283. As REE USA knows, REE Automotive has also supplied REE USA with the stolen OSR trade secrets to market, develop, and sell its products incorporating those trade secrets, and enter into partnerships and raise funds using those trade secrets, in Texas.

284. Thus, REE USA has engaged in acts in furtherance of REE's misappropriation of the stolen OSR trade secrets at the direction of, on behalf of, and for the benefit of REE Automotive as REE Automotive's agent.

COUNT I: VIOLATION OF THE DEFEND TRADE SECRETS ACT

285. OSR incorporates paragraphs 1 through 284 of its Complaint as if fully set forth herein.

286. OSR is the owner of certain valuable trade secrets contained in and relating to its EVOLVER platform, a product which OSR uses and intends to use in interstate and foreign commerce, including trade secrets relating at least to: (i) artificial intelligence, data-as-a-service functionality, and data analytics; (ii) data collection and processing; (iii) data storage and transfer; (iv) universal adaptability; (v) command functions and actuation; (vi) cybersecurity; (vii) functional safety and regulatory compliance; (viii) thermal management; (ix) unique software tools for OEM customers; (x) customer, supplier and component information; (xi) hardware and software architecture for a multi-domain "central brain," and (xii) other trade secrets

287. OSR has taken reasonable steps to maintain the secrecy of its trade secrets, including by, among other things: (i) requiring confidentiality and/or nondisclosure agreements to be signed by any party granted access to OSR's trade secrets; (ii) requiring the use of passwords,

and limiting the access afforded by such passwords based on the nature of each employee's role; (iii) maintaining trade secret information on a closed and secured dedicated computer server that is not connected to the internet or to OSR's open internal network; (iv) physically locking computer terminals in metal cages, which can only be opened by OSR's IT team with proper authorization; (v) requiring multiple levels of review to transfer trade secret information onto devices with internet connectivity; and (vi) restricting physical access to its offices to employees with NFC tags and visitors with prior written authorization who provide identification to security. These confidential and proprietary trade secrets are of substantial economic value and have conferred a competitive advantage on OSR.

288. OSR has not consented, and does not consent, to the use of any of its trade secrets by anyone other than authorized employees as required to perform their duties for OSR.

289. OSR's trade secrets derive independent economic value, actual and potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

290. As discussed herein, based on the stolen files Stauber stole from OSR for REE, the knowledge of the Former Employees, and publicly available information regarding the REE Platform, including the REEcenter, REE has misappropriated OSR's trade secrets, and threatens to continue to misappropriate OSR's trade secrets.

291. Upon information and belief, REE misappropriated and threatens to continue to misappropriate additional OSR trade secrets, which will be identified in discovery.

292. REE misappropriated, and threatens to continue to misappropriate, OSR's trade secrets using the improper and unlawful methods set forth herein. REE's misappropriation of OSR's trade secrets was willful and malicious because, among other reasons and as described

herein, REE knew that the trade secrets were derived from OSR and retained and used them in spite of OSR's demands that REE cease doing so. REE has attempted, and continues to attempt, to conceal its misappropriation and to obstruct OSR's efforts to remedy the misappropriation.

293. Additionally, REE is liable for the Former Employees' misappropriation of trade secrets, pursuant to the doctrine of respondeat superior, because REE knew, or should have known, that its employees misappropriated OSR's trade secrets, but took no steps to end their misappropriation. Rather, REE made use of, and continues to make use of, trade secrets misappropriated by the Former Employees. REE further knew or had reason to know the Former Employees were using OSR's trade secrets in copying OSR's technology for REE, and had either used improper means to acquire those trade secrets and/or owed OSR a duty to maintain the trade secrets' secrecy and limit their use. Indeed, REE recruited the Former Employees for this purpose.

294. Through alter ego liability, REE Automotive, REE Holding, and REE USA are liable for misappropriating OSR's trade secrets. REE Automotive, REE Holding, and REE USA are alter egos of each other because they (i) are controlled by a common group of individuals, (ii) share a common pool of employees who perform services for each other and acts as a single team, (iii) pay for each other's expenses, (iv) fail to maintain corporate formalities, (v) were incorporated by the same people, (vi) lack independent business discretion, and (vii) are in the same line of business.

295. REE Automotive, REE Holding, and REE USA have acted in concert as a single entity in order to conduct business in the United States in furtherance of their misappropriation of OSR's trade secrets. REE Automotive has used REE Holding and REE USA to commit fraud or injustice and to achieve inequitable results, including to avoid the jurisdiction of United States courts and circumvent the DTSA, TUTSA, and other laws, thereby harming OSR. Additionally,

REE Holding and REE USA operate solely as tools or business conduits for REE Automotive in the United States. Further, REE Automotive has purposely left REE USA and REE Holding without assets to satisfy any judgment for its acts within the United States; SEC filings state that "because a majority of our assets and most of our directors and executive officers are located outside of the United States, any judgment obtained in the United States against us or any of them may be difficult to collect within the United States."

296. OSR has no adequate remedy at law. An injunction is necessary to prevent REE's ongoing misappropriation of OSR's trade secrets. Unless REE is enjoined, REE will continue to misappropriate OSR's trade secrets by using the stolen OSR trade secrets in the REE Platform, including in the REEcenter, without authority, and will disseminate OSR's trade secrets to other third parties, including development partners, who have no right to access or use OSR's trade secrets.

297. As the direct and proximate result of REE's conduct, OSR has suffered and continues to suffer irreparable harm and damages of at least $2.6 billion. Among other things, REE's misappropriation of OSR's trade secrets has damaged the market for OSR's EVOLVER platform and trade secrets, and decreased the licensing value of, as well as the licensing of, the trade secrets. REE has been unjustly enriched by its misappropriation of the stolen OSR trade secrets because REE has obtained investments based upon its incorporation of the stolen OSR trade secrets in the REE Platform and has avoided, at minimum, years and billions of dollars of research and development costs, enabling it to gain a significant head start in entering the market with its REE Platform.

298. In addition to equitable relief, OSR demands (i) monetary damages in an amount no less than $2.6 billion, (ii) exemplary damages in an amount two times the amount of

compensatory damages (i.e., no less than $5.2 billion) pursuant to 18 U.S.C. § 1836(b)(3)(C) because REE's misappropriation was willful and malicious, and (iii) attorneys' fees pursuant to 18 U.S.C. § 1836(b)(3)(D) because REE's misappropriation was willful and malicious.

COUNT II: VIOLATION OF THE TEXAS UNIFORM TRADE SECRETS ACT

299. OSR incorporates paragraphs 1 through 298 of its Complaint as if fully set forth herein.

300. OSR is the owner of certain valuable trade secrets contained in and relating to its EVOLVER platform, including trade secrets, as discussed herein, relating at least to: (i) artificial intelligence, data-as-a-service functionality, and data analytics; (ii) data collection and processing; (iii) data storage and transfer; (iv) universal adaptability; (v) command functions and actuation; (vi) cybersecurity; (vii) functional safety and regulatory compliance; (viii) thermal management; (ix) unique software tools for OEM customers; and (x) customer, supplier and component information; (xi) hardware and software architecture for a multi-domain "central brain," and (xii) other trade secrets.

301. OSR has taken reasonable steps to maintain the secrecy of its trade secrets, including by, among other things: (i) requiring confidentiality and/or nondisclosure agreements to be signed by any party granted access to OSR's trade secrets; (ii) requiring the use of passwords, and limiting the access afforded by such passwords based on the nature of each employee's role; (iii) maintaining trade secret information on a closed and secured dedicated computer server that is not connected to the internet or to OSR's open internal network; (iv) physically locking computer terminals in metal cages, which can only be opened by OSR's IT team with proper authorization; (v) requiring multiple levels of review to transfer trade secret information onto devices with internet connectivity; and (vi) restricting physical access to its offices to employees with NFC tags and visitors with prior written authorization who provide identification to security.

These confidential and proprietary trade secrets are of substantial economic value and have conferred a competitive advantage on OSR.

302. OSR has not consented, and does not consent, to defendants' use of any of its trade secrets.

303. OSR's trade secrets derive independent economic value, actual and potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

304. As discussed herein, based on the stolen files Stauber stole from OSR for REE, the knowledge of the Former Employees, and publicly available information regarding the REE Platform and REEcenter, REE has misappropriated OSR's trade secrets, and threatens to continue to misappropriate OSR's trade secrets.

305. Upon information and belief, REE misappropriated, and threatens to continue to misappropriate additional, OSR trade secrets, which will be identified in discovery.

306. REE misappropriated, and threatens to continue to misappropriate, OSR's trade secrets using the improper and unlawful methods set forth herein. REE's misappropriation of OSR's trade secrets was willful and malicious because, among other reasons and as described herein, REE knew that the trade secrets were derived from OSR and retained and used them in spite of OSR's demands that REE cease doing so. REE has attempted, and continues to attempt, to conceal its misappropriation and to obstruct OSR's efforts to remedy the misappropriation.

307. Additionally, REE is liable for the Former Employees' misappropriation of trade secrets, pursuant to the doctrine of respondeat superior, because REE knew, or should have known, that its employees misappropriated OSR's trade secrets, but took no steps to end their misappropriation. Rather, REE made use of, and continues to make use of, trade secrets

misappropriated by the Former Employees. REE further knew or had reason to know the Former Employees were using OSR's trade secrets in copying OSR's technology for REE, and had either used improper means to acquire those trade secrets and/or owed OSR a duty to maintain the trade secrets' secrecy and limit their use. Indeed, REE recruited the Former Employees for this purpose.

308. Additionally, through alter ego liability, REE Automotive, REE Holding, and REE USA are liable for misappropriating OSR's trade secrets. REE Automotive, REE Holding, and REE USA are alter egos of each other because they (i) are controlled by a common group of individuals, (ii) share a common pool of employees who perform services for each other and acts as a single team, (iii) pay for each other's expenses, (iv) fail to maintain corporate formalities, (v) were incorporated by the same people, (vi) lack independent business discretion, and (vii) are in the same line of business.

309. REE Automotive, REE Holding, and REE USA have acted in concert as a single entity in order to conduct business in the United States in furtherance of their misappropriation of OSR's trade secrets. REE Automotive has used REE Holding and REE USA to commit fraud or injustice and to achieve inequitable results, including to avoid the jurisdiction of United States courts and circumvent the DTSA, TUTSA, and other laws, thereby harming OSR. Additionally, REE Holding and REE USA operate solely as tools or business conduits for REE Automotive in the United States. Further, REE Automotive has purposely left REE USA and REE Holding without assets to satisfy any judgment for its acts within the United States.

310. OSR has no adequate remedy at law. An injunction is necessary to prevent REE's ongoing misappropriation of OSR's trade secrets. Unless REE is enjoined, REE will continue to misappropriate OSR's trade secrets by using the stolen OSR trade secrets in the REE Platform, including in the REEcenter, without authority, and will disseminate OSR's trade secrets to other

third parties, including development partners, who have no right to access or use OSR's trade secrets.

311. As the direct and proximate result of REE's conduct, OSR has suffered and continues to suffer irreparable harm and damages of at least $2.6 billion. Among other things, REE's misappropriation of OSR's trade secrets has damaged the market for OSR's EVOLVER platform and trade secrets, and decreased the licensing value of, as well as the licensing of, the trade secrets. REE has been unjustly enriched by its misappropriation of the stolen OSR trade secrets because REE has obtained investments based upon its incorporation of the stolen OSR trade secrets in the REE Platform and has avoided, at minimum, years and billions of dollars of research and development costs, enabling it to gain a significant head start in entering the market with its REE Platform.

312. In addition to equitable relief, OSR demands (i) monetary damages in an amount no less than $2.6 billion, (ii) exemplary damages in an amount two times the amount of compensatory damages (i.e., no less than $5.2 billion) pursuant to Tex. Civ. Prac. & Rem. Code § 134A.004(b) because REE's misappropriation was willful and malicious, and (iii) attorneys' fees pursuant to Tex. Civ. Prac. & Rem. Code § 134A.005(3) because REE's misappropriation was willful and malicious.

COUNT III: UNFAIR COMPETITION—MISAPPROPRIATION

313. OSR incorporates paragraphs 1 through 312 of its Complaint as if fully set forth herein.

314. OSR created confidential information in connection with its development of EVOLVER and the underlying technology. To do so required an original idea, and a significant investment of time, labor, employee expertise and money.

315. OSR's confidential information, independently and to the extent not considered a trade secret, relates, among other things, at least to: (i) artificial intelligence and data analytics; (ii) data collection and processing; (iii) data storage and transfer; (iv) universal adaptability; (v) command functions and actuation; (vi) cybersecurity; (vii) functional safety and regulatory compliance; (viii) thermal management; (ix) unique software tools for OEM customers; (x) customer, supplier and component information; (xi) hardware and software architecture for a multi-domain "central brain," and (xii) other confidential information.

316. REE has used that confidential information to compete with OSR, gaining a special advantage because it was not required to create an original idea or to make a similar investment to develop the same technology. Instead, REE announced that it would be producing products with similar technology within a drastically shorter period of time than it would take to develop that technology. REE was only able to do so as a result of to REE's theft and accessing of OSR's confidential information.

317. Through alter ego liability, REE Automotive, REE Holding, and REE USA are liable for misappropriating OSR's confidential information. REE Automotive, REE Holding, and REE USA are alter egos of each other because they (i) are controlled by a common group of individuals, (ii) share a common pool of employees who perform services for each other and acts as a single team, (iii) pay for each other's expenses, (iv) fail to maintain corporate formalities, (v) were incorporated by the same people, (vi) lack independent business discretion, and (vii) are in the same line of business.

318. REE Automotive, REE Holding, and REE USA have acted in concert as a single entity in order to conduct business in the United States in furtherance of their misappropriation of OSR's confidential information. REE Automotive has used REE Holding and REE USA to

commit fraud or injustice and to achieve inequitable results, including to avoid the jurisdiction of United States courts and circumvent the DTSA, TUTSA, and other laws, thereby harming OSR. Additionally, REE Holding and REE USA operate solely as tools or business conduits for REE Automotive in the United States. Further, REE Automotive has purposely left REE USA and REE Holding without assets to satisfy any judgment for its acts within the United States; SEC filings state that "because a majority of our assets and most of our directors and executive officers are located outside of the United States, any judgment obtained in the United States against us or any of them may be difficult to collect within the United States."

319. OSR has no adequate remedy at law. An injunction is necessary to prevent REE's ongoing misappropriation of OSR's confidential information. Unless REE is enjoined, REE will continue to misappropriate OSR's confidential information by using the stolen OSR confidential information in the REE Platform, including in the REEcenter, without authority.

320. OSR suffered competitive harm as a result of REE's misappropriation of its confidential information, in an amount to be determined at trial, but no less than $2.6 billion. Additionally, OSR is entitled to exemplary damages because REE committed acts amounting to fraud, malice, and gross negligence and demonstrated specific intent to cause substantial injury or harm to OSR.

COUNT IV: INJUNCTIVE RELIEF

321. OSR incorporates paragraphs 1 through 320 of its Complaint as if fully set forth herein.

322. As set forth in the First, Second, and Third Counts, *supra*, REE has violated the DTSA and the TUTSA, misappropriating OSR's trade secrets and confidential information. There is thus a strong likelihood that OSR will succeed on its claims in this action.

323. REE's misconduct has caused, and continues to cause, OSR injury, including, without limitation, irreparable harm for which there is no adequate remedy at law, including at least increased market competition because of REE's use of OSR's trade secrets and confidential information and likely destruction of OSR's trade secrets as a result of REE's unauthorized disclosure to its employees and partners. (*See supra* at ¶¶ 270, Part VI.B.)

324. There is no adequate remedy at law to compensate OSR for the irreparable harm caused by REE's misappropriation of its trade secrets and confidential information.

325. To protect OSR from such irreparable harm, the Court should order that REE, directly or indirectly, and whether alone or in concert with others, be preliminarily and permanently enjoined from: (i) inducing or permitting any current or former OSR employees to disclose any of OSR's trade secrets or confidential information; (ii) accessing, using, imitating, copying, disclosing, or making available to any person or entity any of OSR's trade secrets or confidential information, including using OSR's trade secrets or confidential information in any of REE's products or prototypes; (iii) interfering with the Employment and Secrecy Agreements between OSR and any of its current or former employees; or (iv) deleting or otherwise destroying, concealing, or altering any of OSR's trade secrets or confidential information. Further, the Court should order the seizure and return of all documents or information in the possession of REE and REE's agents that concern or relate to OSR's trade secrets or confidential information and the disclosure of any and all persons or entities to whom REE has disclosed one or more of OSR's trade secrets or confidential information, or whom REE knows to be in possession of one or more of OSR's trade secrets or confidential information, to OSR.

326. The balance of equities strongly favors issuing injunctive relief in favor of OSR, as REE will suffer no hardship from being ordered to cease and desist from committing continued

unlawful acts and, specifically, from gaining unauthorized access to and making unauthorized use of OSR's trade secrets or confidential information. Nor will REE suffer any hardship from being required to return any of OSR's trade secrets or confidential information in its possession.

327. An injunction will not adversely affect the public interest. To the contrary, injunctive relief will benefit the public interest because the public has an interest in preventing conduct that violates the laws of the United States and Texas, including specifically the misappropriation of trade secrets.

JURY DEMAND

328. OSR hereby requests a trial by jury pursuant to Rule 38 of the Federal Rules of Civil Procedure.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request the Court:

A. Enter a judgment in favor of OSR and against REE on all of OSR's claims asserted in this Complaint;

B. Issue an injunction preliminarily and permanently enjoining REE and its agents, employees, attorneys, successors and assigns, and all persons, firms and corporations acting in concert with it, from:

1. inducing or permitting any current or former OSR employees to disclose any of OSR's trade secrets;

2. accessing, using, imitating, copying, disclosing, or making available to any person or entity any of OSR's trade secrets, including using OSR's trade secrets in any of REE's products or prototypes;

3. interfering with the Employment and Secrecy Agreements between OSR and any of its current or former employees; or

4. deleting or otherwise destroying, concealing, or altering any of OSR's trade secrets;

C. Compel REE to take affirmative actions to protect OSR's trade secrets, including, without limitation:

1. a seizure and return of all documents or information in REE's possession that

concern or relate to OSR's trade secrets,

2. disclosure of any and all persons or entities to whom REE has disclosed one or more of OSR's trade secrets, or whom REE knows to be in possession of one or more of OSR's trade secrets, to OSR;

D. Establish a constructive trust, and require REE to transfer legal title to OSR of any and all intellectual property, devices, machines, software, documents, or other objects or data that were developed or created using OSR's trade secrets and confidential information;

E. Award OSR monetary damages, both compensatory and punitive, including exemplary damages pursuant to 18 U.S.C. § 1836(b)(3)(C) and Tex. Civ. Prac. & Rem. Code § 134A.004(b), as a result of each cause of action against REE, including, but not limited to, damages as a result of REE's misappropriation of OSR's trade secrets under the DTSA and state law, all in amounts to be determined at trial, plus interest;

F. Award OSR all expenses for this action, including costs and attorneys' fees, pursuant to 18 U.S.C. § 1836(b)(3)(D) and Tex. Civ. Prac. & Rem. Code § 134A.005(3);

G. Award to OSR pre-judgment and post-judgment interest on all damages awarded; and

H. Award such other and further relief as the Court may deem just and proper.

Dated: December 16, 2022
Houston, Texas

Respectfully submitted,

KASOWITZ BENSON TORRES LLP

/s/ Constantine Z. Pamphilis

Constantine Z. Pamphilis
Attorney in Charge
Texas State Bar No. 00794419
WDTX Bar No. 00794419
DPamphilis@kasowitz.com
1415 Louisiana Street, Suite 2100
Houston, Texas 77002
Telephone: (713) 220-8800
Facsimile: (713) 222-0843

Marc E. Kasowitz (*pro hac vice forthcoming*)
MKasowitz@kasowitz.com
Paul J. Burgo (*pro hac vice forthcoming*)
PBurgo@kasowitz.com
Daniel J. Koevary (*pro hac vice forthcoming*)
DKoevary@kasowitz.com
Rachel Bandli (*pro hac vice forthcoming*)
RBandli@kasowitz.com
1633 Broadway
New York, New York 10019
Telephone: (212) 506-1700
Facsimile: (212) 506-1800

Attorneys for Plaintiffs OSR ENTERPRISES AG and OSR R&D ISRAEL LTD.